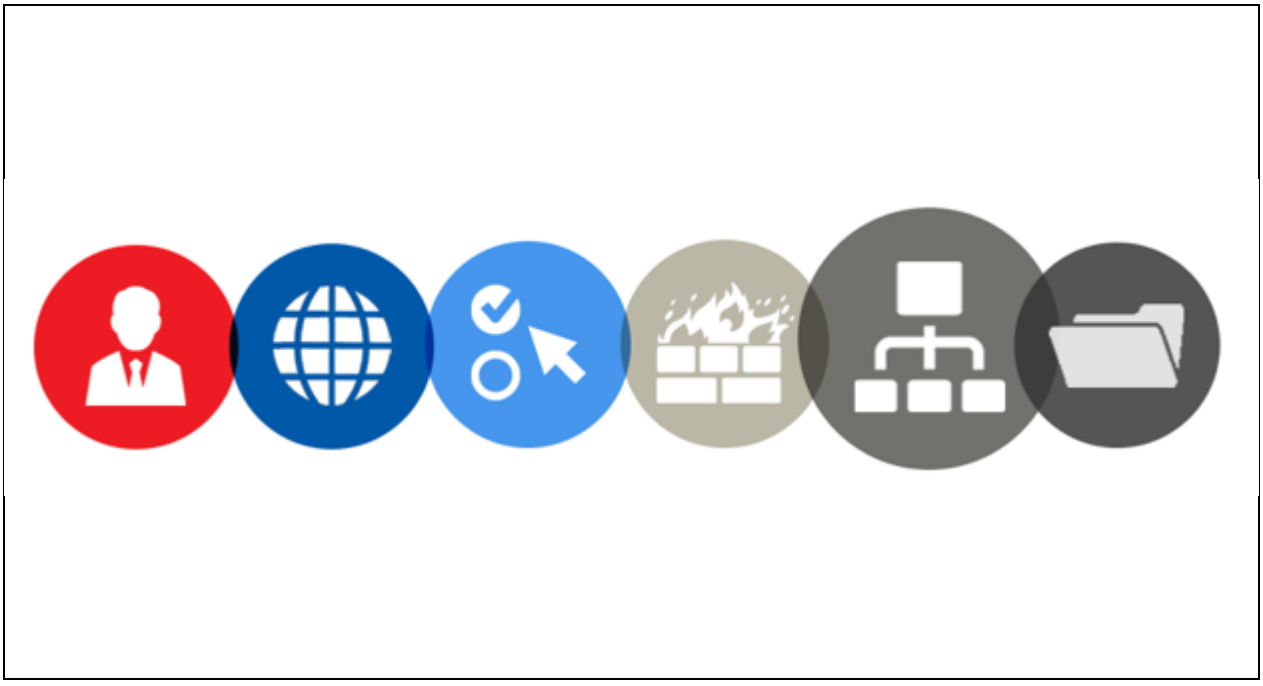
Haute Ecole de Gestion & Tourisme
Hochschule für Wirtschaft & Tourismus

Filière Informatique de gestion
Studiengang Wirtschaftsinformatik

Travail de Bachelor 2018

Intégration de la RGPD et de la nouvelle LPD auprès des Instituts de « Recherche et Développement » de la HES-SO Valais



Étudiant : Patrick Clivaz

Professeur : Bruno Montani

Déposé le : 30 juillet 2018

HES-SO Valais-Wallis • rue de la Plaine 2 • 3960 Sierre
+41 27 606 89 11 • info@hevs.ch • www.hevs.ch

RÉSUMÉ

La Haute École Spécialisée de Suisse occidentale (HES-SO) m'a demandé, par le professeur M. Bruno Montani, de réaliser un prototype d'outil d'aide pour la mise en conformité de la RGPD et de la LPD auprès des instituts.

Durant ce travail, des recherches et analyses approfondies ont, dans un premier temps, été effectuées pour présenter l'état des différents textes légaux européen et suisse.

Dans un deuxième temps, des outils d'accompagnements aux entreprises déjà disponibles ont été testés et analysés afin d'évaluer leur manière de fonctionner et leur utilité.

Le type d'outil et les langages de développement ont ensuite été explorés afin de sélectionner les technologies les plus adaptées à la réalisation de l'outil.

Le développement de l'outil a principalement constitué la dernière phase de travail. Une multitude d'uses cases y ont été implémentés afin que l'utilisateur puisse tester au mieux ce prototype. Il est accessible dans un navigateur web et permet à l'utilisateur d'obtenir différentes recommandations selon des réponses données dans un formulaire.

MOTS CLÉS

Travail de Bachelor, Protection des données, Loi, Analyse, PHP

AVANT-PROPOS

Dans le cadre du travail de Bachelor, réalisé lors du 6e semestre de la filière Informatique de Gestion à la HES-SO Valais-Wallis, et proposé par le professeur Bruno Montani, l'étudiant a reçu la tâche d'effectuer une analyse sur les lois « Règlement Général sur la protection des Données » (partie européenne) et « Loi sur la Protection des Données » (partie suisse) ainsi que de réaliser un outil qui facilitera la mise en conformité de ces lois dans le cadre de la HES-SO Valais, principalement dans le contexte des Instituts de Recherche et Développement.

Au vu des changements légaux récents, aucun outil allant dans ce sens n'existe actuellement au sein des instituts la HES-SO Valais et la gestion des données selon les principes du RGPD et du projet de révision de la LPD n'est pas certaine d'être assurée.

L'objectif principal de ce travail de Bachelor est donc d'analyser les principaux articles de ces deux lois afin de cibler les ajustements essentiels que devront réaliser les instituts de la HES-SO Valais pour assurer leur conformité dans les plus brefs délais.

Afin d'aider le DPO pour sa prise de décisions relatives aux projets des instituts, un prototype, basé sur les outils existants d'accompagnement aux entreprises, est donc réalisé afin de démontrer le fonctionnement qu'un tel outil pourrait impliquer.

REMERCIEMENTS

Je tiens à remercier toutes les personnes qui m'ont permis de réaliser ce travail de Bachelor dans des conditions optimales.

Spécialement à :

M. Bruno Montani, mon professeur responsable, pour m'avoir encadré et suivi durant toutes les étapes de la réalisation de ce travail. Merci pour ses recommandations, sa disponibilité et son implication.

M. Adriano Labate, responsable de la sécurité des Systèmes d'Information (RSSI) au Groupe T2i, pour avoir accepté de me rencontrer afin de discuter des divers processus de mise en conformité légaux et des impacts aux changements juridiques dans une importante entreprise informatique.

M. Alexandre Cotting, collaborateur à l'Institut d'Informatique de Gestion (IIG) de la HES-SO Valais-Wallis et M. Francesco Cimmino, assistant de recherche à l'Institut Entrepreneuriat & Management (IEM) de la HES-SO Valais-Wallis pour leurs retours et suggestions d'une vision purement relative aux instituts liés à l'outil.

Mme Natacha Albrecht, conseillère juridique de la HES-SO Valais-Wallis pour la mise à disposition de son mémoire ainsi que ses précieux conseils et corrections concernant les textes de loi suisse et européen.

M. Pedro Gil Ferreira pour ses conseils lors de l'implémentation PHP afin de réaliser simplement une structure *MVC*.

Enfin, merci aux personnes ayant pris le temps de relire ce rapport.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

CD	Disque compact
CNIL	Commission Nationale de l'Informatique et des Libertés
CRM	Customer Relationship Management - Gestion de la Relation Client
CSS	Cascading Style Sheets – Feuilles de Style en Cascades
CUI Unige	Centre Universitaire d'Informatique de l'Université de Genève
DPA	Data Protection Authority – Autorité de Protection des Données
DPO	Data Protection Officier – Délégué à la Protection des Données
EPFL	École polytechnique fédérale de Lausanne
ERP	Enterprise Ressource Planning - Progiciel de gestion intégré
GDPR	General Data Protection Regulation
HES-SO	Haute École Spécialisée de Suisse Occidentale
HTML	HyperText Markup Language – Langage de balises pour l'hypertexte
IAPP	Association internationale des professionnels de la protection de la vie privée
IDE	Integrated Development Environment – Environnement de Développement Intégré
IIG	Institut Informatique de Gestion
IEM	Institut de Recherche Entrepreneuriat & Management
JS	JavaScript
LIPDA	Loi sur l'information, la Protection des Données et l'Archivage
LPD	Loi sur la Protection des Données
MVC	Model-View-Controller – Modèle Vue Contrôleur
OCPD	Ordonnance sur les Certifications en matière de Protection des Données
OLPD	Ordonnance relative à la Loi fédérale sur la Protection des Données
PFPDT	Préposé fédéral à la Protection des Données et à la Transparence
PHP	PHP Hypertext Preprocessor
PIA	Privacy Impact Assessment - Évaluation des facteurs relatifs à la vie privée
Ra&D	Recherche et Développement
RH	Ressources Humaines
RF	Responsable de Filière
RGPD	Règlement Général sur la Protection des Données
SaaS	Software as a Service – Logiciel en tant que service
SQL	Structured Query Language – Langage de requête structuré
UE	Union européenne
XAMPP	XAMPP Apache + MysqlDB + PHP + Perl

INTRODUCTION

Contexte général

Un cadre légal autour de la sécurité des systèmes d'information n'a jamais clairement été défini pour diverses raisons. Ce flou a longtemps permis aux différentes entreprises de gérer cette sécurité de manière aléatoire.

En 2016, la nouvelle Règlementation européenne pour la Protection des Données (RGPD) est entrée en vigueur et les entreprises concernées ont eu l'obligation de se mettre en conformité. La Suisse a emboîté le pas de l'Union européenne en entamant une révision de la Loi sur la Protection des Données (LPD).

Le cadre règlementaire suisse actuel, basé sur la loi du 1er juin 1992, définit déjà un certain nombre de concepts et de règles qui servent aussi de base à la nouvelle règlementation européenne. Néanmoins, de nouvelles règles apparaissent et les nombreuses subtilités pourraient avoir des impacts importants sur les activités des entreprises.

Problématique concrète

Au vu de ces changements légaux en Europe et en Suisse, une analyse fine des adaptations auxquelles les entreprises vont devoir faire face ces prochains mois est nécessaire. Quasiment toutes les entreprises suisses traitent, de manière informatisée ou non, des données qui tombent sous la loi européenne, respectivement suisse.

Malheureusement, la majorité des entreprises ne possèdent pas les moyens et/ou compétences pour se mettre en conformité avec ces lois, tant sous l'aspect technique que procédural.

La HES-SO Valais n'échappe pas à ces lois et ce travail vise à lui offrir un outil d'aide à son DPO pour les différentes étapes à suivre, définies selon le contexte, le périmètre géographique (UE ou Suisse) ainsi que l'utilisation précise des données afin qu'elle puisse se mettre en conformité avec ces deux lois majeures.

Outil développé

L'outil développé doit comporter une interface visuelle pour l'utilisateur. Cette interface offrira la possibilité à l'utilisateur de sélectionner différents critères : un lab, un type de données et un responsable de traitement. Il pourra ainsi répondre à diverses questions émanant des principes relatifs à la protection des données. L'utilisateur, qui sera le DPO, verra ensuite s'afficher un récapitulatif des données qu'il a insérées et des résultats par périmètres légaux en fonction de ses choix.

Déliverables

Les déliverables disponibles sur le CD en annexe de ce dossier sont les suivants :

- Le rapport final
- Les uses cases réalisés
- Un guide pour une installation locale
- Le mémoire de Mme Natacha Albrecht
- L'outil développé
- Le poster de présentation

1. État de l'Art juridique

La loi européenne et son pendant suisse sont actuellement en pleine transformation afin de suivre les évolutions numériques récentes. Ainsi, la manière de gérer les aspects relatifs à la protection des données a été redéfinie précisément dans ses deux textes, remis au goût de jour récemment.

Cet État de l'Art a été écrit avec le support des différents textes légaux et des recommandations d'avocats spécialisés. (Assemblée fédérale de la Confédération suisse, 1992) (Confédération Suisse, 2017) (Kellerhals Carrard, 2017) (Parlement européen et Conseil relatif à la protection des personnes physiques, 2018)

Le mémoire réalisé dans ce sens par Mme Natacha Albrecht, juriste auprès de la HES-SO Valais a également servi de base solide, principalement pour la partie suisse. (Albrecht, 2018)

1.1. RGPD (partie européenne)

Le Règlement européen sur la protection des données (RGPD) est un règlement qui a pour but de renforcer et d'unifier la protection des données de tous les citoyens européens. Il a été définitivement adopté par le parlement européen le 14 avril 2016 et est en application depuis le 25 mai 2018.

Ce règlement remplace la directive sur la protection des données personnelles datant de 1995.

Figure 1 : Principaux points du RGPD

Source : (econocom, 2018)

1.1.1. Définitions

Avant de détailler le RGPD, il est important de prendre en compte les définitions ci-dessous mentionnées dans ledit texte (Parlement européen et Conseil relatif à la protection des personnes physiques, 2018) :

- « données à caractère personnel », toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

- « traitement », toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

- « profilage », toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

- « pseudonymisation », le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

- « fichier », tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

- « responsable du traitement », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

- « sous-traitant », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

- « tiers », une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel;

- « consentement » de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

- « violation de données à caractère personnel », une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données;

- « données génétiques », les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

- « données biométriques », les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;

- « données concernant la santé », les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne;

- « entreprise », une personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique;

1.1.2. Principes de la protection des données

Il est important de prendre en compte que la RGPD définit seulement le traitement des données comme traitement automatisé. Si un traitement manuel est effectué, il n'y est pas soumis, sauf si ce traitement est informatisé et effectué régulièrement. Afin de s'assurer d'être en conformité totale avec cette loi, les entreprises doivent rester particulièrement attentives aux devoirs suivants.

Information et consentement donnés clairement à la personne concernée

Si elle n'a pas accepté formellement et librement le traitement de ses données personnelles, il est purement interdit de les collecter. Cette procédure doit être appliquée systématiquement et indépendamment du type de données (sensibles ou personnelles). Pour cela, elle doit avoir un choix réel de l'accepter ou non, une alternative doit exister, le consentement ne peut plus être présumé. Elle doit aussi être informée du but précis et du type de données collectées. L'entreprise doit divulguer des informations pertinentes et suffisamment concrètes. Il doit y avoir une finalité spécifique pour chaque donnée, la personne doit savoir à quoi cela va servir. Ce consentement peut être transmis sous forme électronique ou orale et ne doit pas avoir une forme particulière. Son approbation doit dans tous les cas être donné explicitement, une case précochée ne peut par exemple pas être utilisée. De la même manière que le consentement, la révocation de celui-ci doit pouvoir être possible à tout moment.

Assurer le « Privacy by design » et le « Privacy by default »

Ces deux concepts permettent une protection des données par des moyens purement techniques. L'objectif est d'instaurer une culture de protection des données à l'interne de l'entreprise. La notion de « Privacy by design » vise à prévenir les risques avant même le traitement de ces données et réduit ainsi le risque d'atteinte à la personnalité et de violation des droits fondamentaux. Cela est défini par une suppression régulière de données non primordiales ainsi que leur anonymisation (ou pseudonymisation) systématique. Le principe de la minimisation des données est donc appliqué, seulement les données nécessaires seront ainsi utilisées. Le concept « Privacy by default » permet de s'assurer à l'aide de paramètres définis par défaut que seules les données personnelles nécessaires seront traitées pour la finalité prévue. En respectant cela, une entreprise doit par exemple permettre d'effectuer des achats en ligne sans pour autant « forcer » l'utilisateur à se rattacher à un profil client.

Désignation d'un représentant dans l'UE

La nomination d'un responsable de traitement de données (DPO) ou d'un mandat à l'externe devient quasiment obligatoire. Cela peut également passer par une filiale qui possède un siège social au sein de l'UE, si son siège principal ne s'y trouve pas.

Tenir un registre des activités de traitement

Après avoir déterminé dans quelles circonstances des données de clients, fournisseurs ou employés seront collectées et/ou traitées, il est nécessaire de lister les applications et outils utilisés par les systèmes d'information de l'entreprise pour le stockage de ces données et « tracer » cela dans un registre. Cette mesure est obligatoire si la barre des 250 employés au sein de l'entreprise est dépassée.

Obligation de notifier une violation de données personnelles

Le responsable de traitement de données est soumis à notifier toute violation à l'autorité de contrôle compétente (DPA) dans un délai de 72 heures si cette violation est susceptible d'engendrer un risque pour les droits et libertés. Il faut aussi relever que la ou les personnes concernées par cette violation doivent également être notifiées.

Analyser l'impact relatif à la protection des données

Ce principe est basé sur l'autorégulation. Une entreprise doit être conforme à la protection des données en tout temps et pouvoir le prouver. Si les droits et libertés des personnes physiques ne peuvent être respectés, l'autorité de contrôle doit être consultée afin de trouver une solution.

Quelques précisions supplémentaires sont également présentes dans ce nouveau texte. Ainsi, les données qui peuvent être considérées comme ultra-sensibles (registre des condamnations pénales par exemple) ne peuvent être traitées que sous contrôle d'une autorité publique ou en accord avec le droit de l'état.

Les notions de « droit à l'oubli » et « droit à la rectification » font également leurs apparitions. Une personne concernée pourra en tout temps exiger que le responsable de traitements efface ses données personnelles et cesse la diffusion de celles-ci. Cela concerne également l'effacement de tout lien vers les données et de toutes les éventuelles copies ou reproductions de celles-ci.

Enfin, le « droit à la portabilité des données » est introduit dans ce nouveau texte. Il permettra à la personne concernée de transférer facilement ses données entre différents services concurrents. Par exemple, les données de services de streaming musicaux (playlists, goûts musicaux, historique d'écoute), d'application de santé (rythme cardiaque, durée d'exercices et localisations des activités physiques) ou d'hébergeurs en ligne (fichiers stockés) devront pouvoir être facilement déplacées entre les différents serveurs et effacées de l'ancien service.

1.1.3. Champs d'application

En règle générale, le champ d'application peut-être très large, et il concerne principalement toutes les personnes qui se trouvent sur le territoire de l'Union européenne.

Naturellement, les entreprises y sont directement impactées et le fait qu'elles soient établies en Europe et qu'elles exercent une activité stable est un critère déterminant et cela indépendamment de leur forme juridique. En outre, dans le cas où leur siège principal ne se situerait pas au sein de l'UE, elles sont aussi concernées si elles effectuent ces deux actions de traitement au sein du territoire de l'UE.

1. **Offre de biens ou services à leurs utilisateurs** : il est important de mentionner qu'un paiement exigé ou non n'y change rien. Le critère déterminant pour prouver cela est l'utilisation par ces entreprises d'une langue ou d'une monnaie utilisée couramment dans un ou des États membres de l'UE. Ce critère présume une intention d'offrir des biens ou services à des citoyens de l'UE,
2. **Suivi du comportement des utilisateurs (traçabilité)** : cet élément est applicable à partir du moment où l'activité de l'utilisateur est tracée (à l'aide d'un outil comme *Google Analytics*[1] par exemple) et/ou des techniques de profilage de personnes physiques permettent d'analyser, de prédire des goûts, d'évaluer de futurs comportements ou de déterminer des habitudes (au moyen de cookies).

1.1.4. Sanctions en cas de violation

Les sanctions auxquelles s'engagent les entreprises ne respectant pas ces devoirs peuvent s'avérer très lourdes en conséquence. Il est utile de préciser que ces sanctions sont uniquement civiles. Pour le pénal, chaque État membre pourra définir les sanctions selon sa propre législation.

En effet, une première mesure peut résulter d'une amende administrative qui peut s'élever jusqu'à 4% du chiffre d'affaires annuel et mondial de l'exercice précédent ou d'au maximum 20 millions d'euros. Le montant le plus important sera donc retenu. Il dépendra de différents critères comme la nature, la gravité, l'intentionnalité ou la négligence, les antécédents, le degré de coopération, les catégories de données personnelles concernées ainsi que les circonstances aggravantes ou atténuantes qui en résultent (avantages financiers obtenus ou pertes évitées par la violation).

[1] Service gratuit d'analyse d'audience d'un site Web ou d'applications, https://www.google.com/analytics/

Dans un deuxième temps, les associations de protection des consommateurs auront plus de champs d'action et peuvent faire valoir les droits des personnes affectées par cette violation en introduisant une action judiciaire collective à l'encontre de l'entreprise responsable.

1.2. LPD actuelle

La Loi fédérale sur la Protection des Données (LPD) est une loi fédérale qui vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données dans le territoire suisse.

Cette loi a été approuvée par l'Assemblée fédérale de la Confédération suisse le 19 juin 1992. Elle a été complétée le 14 juin 1994 par l'Ordonnance relative à la Loi fédérale sur la Protection des Données (OLPD) ainsi que le 28 septembre 2007 par l'Ordonnance sur les Certifications en matière de Protection des Données (OCPD).

1.2.1. Définitions

Tout comme pour le texte européen, il est important de prendre en compte ces définitions mentionnées comme suit à l'article 3 de la LPD (Assemblée fédérale de la Confédération suisse, 1992) :

a. données personnelles (données), toutes les informations qui se rapportent à une personne identifiée ou identifiable ;

b. personne concernée, la personne physique ou morale au sujet de laquelle des données sont traitées ;

c. données sensibles, les données personnelles sur :

1. les opinions ou activités religieuses, philosophiques, politiques ou syndicales,

2. la santé, la sphère intime ou l'appartenance à une race,

3. des mesures d'aide sociale,

4. des poursuites ou sanctions pénales et administratives ;

d. profil de la personnalité, un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique ;

e. traitement, toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données ;

f. communication, le fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant ;

g. fichier, tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée ;

h. organe fédéral, l'autorité ou le service fédéral ainsi que la personne en tant qu'elle est chargée d'une tâche de la Confédération ;

i. maître du fichier, la personne privée ou l'organe fédéral qui décide du but et du contenu du fichier ;

1.2.2. Principes de la protection des données

Les données sont en mesure d'être traitées uniquement si leur traitement ne porte pas atteinte à la personnalité.

Le droit fédéral suisse définit 7 principes en matière de protection des données qui doivent impérativement être respectés lors de toute collecte ou traitement de données :

1. **La licéité :** avant de débuter un traitement, il est impératif de vérifier qu'aucune loi ne l'interdise. Si ce n'est pas le cas, les données peuvent alors être traitées. Néanmoins, elles ne peuvent être obtenues par crainte ou usurpation.
2. **La bonne foi :** la récolte de données doit se faire de manière transparente et sincère.
3. **La proportionnalité :** les données collectées doivent seulement être nécessaires et conformes au but entrepris.
4. **La « reconnaisabilité » :** la personne concernée doit pouvoir reconnaître la collecte et le traitement de ses données.
5. **La finalité :** un but précis doit être défini préalablement pour la collecte ainsi que le traitement.
6. **L'exactitude :** les données collectées et traitées doivent être exactes, c'est-à-dire être tenues à jour en tout temps.
7. **La sécurité :** Des mesures techniques et opérationnelles doivent être prises afin d'éviter et de protéger un traitement non autorisé.

Relevons que si une personne privée traite des données sensibles, la personne concernée doit être informée de ce traitement automatiquement. Enfin, cette dernière peut, en tout temps, demander un droit d'accès à ses données. Cette procédure sera, en principe, gratuite et la personne traitant les données aura 30 jours pour y répondre.

1.2.3. Champs d'application

La LPD est applicable aux organes fédéraux ainsi qu'aux personnes privées. Les organismes accomplissant des tâches fédérales y sont également soumis.

Son application ne concerne que le traitement des données, c'est-à-dire toutes les opérations relatives à des données personnelles comme la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de ces données.

La LPD dénombre deux types de données : les données personnelles qui sont les informations correspondant à une personne identifiée ou identifiable et les données sensibles qui concernent les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, les mesures d'aide sociale ainsi que les poursuites ou sanctions pénales et administratives.

1.2.4. Sanctions en cas de violation

Deux infractions sont à distinguer, à savoir la violation des obligations de renseigner, de déclarer et de collaborer avec les personnes privées ainsi que la violation du devoir de discrétion.

La première infraction réprime, uniquement sur plainte, les personnes privées qui vont à l'encontre du droit d'accès aux personnes concernées ou qui refuseraient d'informer lors de la collecte d'informations sensibles ou de profil de la personnalité, en fournissant des renseignements erronés ou incomplets. En cas de communication transfrontalière non déclarée de données au préposé fédéral, une amende est également prévue.

La deuxième infraction réprime, également sur plainte, une révélation intentionnelle de données sensibles ou de profils de la personnalité à autrui de manière illicite. La sanction est la même si une obligation de garder le secret sur ces données avait été définie, même si les rapports de travail ont cessé.

Il est également à signaler que, si une personne détourne des données sensibles non accessibles publiquement, une sanction de peine privative de liberté de maximum 3 ans ou une peine pécuniaire est applicable. Encore une fois, cette sanction est exclusivement applicable à la suite d'une plainte.

1.3. Projet de révision de la LPD

Afin de renforcer les droits des citoyens et face à la révolution numérique, le Conseil Fédéral a adopté un projet de révision totale de cette loi le 15 septembre 2017, après d'intenses discussions débutées en décembre 2011. Ce projet de loi pourrait être appliqué en 2019, voir 2020.

Le but de ce projet est avant tout d'adapter la législation suisse au standard européen. Les données doivent pouvoir être transmises facilement entre la Suisse et les États membres de l'UE. Il faut noter que ces nouvelles dispositions légales ne vont pas au-delà du droit européen, il n'y a pas de « plus » Suisse.

1.3.1. Principales mesures annoncées

Quatre principales mesures ont été annoncées à ce jour par le Conseil Fédéral (Confédération suisse, 2017) :

1. Indépendamment du type de données collectées, tous les particuliers devront désormais être informés lorsqu'une entreprise collecte des données à leur sujet.

2. Dès la mise en place de ces nouveaux traitements, les entreprises seront tenues de prendre en considération tous les enjeux relatifs à la protection des données.

3. Des mesures provisionnelles et des décisions contraignantes pourront être ordonnées par le préposé fédéral à la protection des données, au terme d'une enquête ouverte d'office ou sur dénonciation

4. Les amendes pourront être portées jusqu'à 250'000 CHF au maximum.

1.3.2. Changements à la LPD en vigueur

Cette loi repose désormais principalement sur la gestion réalisée du traitement des données par les personnes privées et non sur le fichier précis qui contient ces données, à la différence de la LPD actuelle. Le poste de responsable du traitement des données (DPO) devient donc primordial pour les entreprises.

En comparaison avec la LPD actuelle, une entreprise qui traite régulièrement des données sensibles ou des profils de personnalité sera ainsi tenue de conserver automatiquement un registre des traitements de données et non plus un registre des fichiers contenant les données. Cette mesure est cependant applicable uniquement si une personne privée emploie plus de cinquante collaborateurs.

Avec ce projet de révision, seules les données traitées en rapport aux personnes physiques seront directement impactées. Ainsi, les données des personnes morales ne sont plus concernées avec cette nouvelle loi.

Des éléments ont également été ajoutés afin de se mettre en conformité avec la numérisation des données. Ainsi les données biométriques et génétiques seront intégrées au terme de « données sensibles ». La notion de « profil », présente dans la LPD actuelle, est remplacée par celle de « profilage ». Cette notion se réfère à toutes les données collectées qui permettent de se faire une idée précise sur les préférences, habitudes et comportements d'une personne.

Étant donné que le traitement de ces données se fait souvent automatiquement, la notion de « traitement automatisé » a été ajoutée.

Le statut et l'indépendance du Préposé fédéral à la protection des données et à la transparence (PFPDT) sont renforcés. Alors qu'il ne peut émettre aujourd'hui que des recommandations aux entreprises, il pourra à l'avenir ordonner des mesures provisionnelles et prendre des décisions contraignantes, au terme d'une enquête ouverte d'office ou sur dénonciation. Il ne pourra toutefois pas décréter de sanction(s) administrative(s). Seuls les tribunaux auront cette prérogative.

Enfin, la notion de DPO est également décrite plus scrupuleusement. Ainsi, sa nomination sera facultative pour les personnes privées, mais obligatoire pour les organes fédéraux. Il est toutefois possible de mandater une entreprise externe spécialisée pour réaliser cette tâche.

1.3.3. Sanctions en cas de violation

Les sanctions définies par ce nouveau projet sont beaucoup plus drastiques et la liste des comportements punissables s'allonge. Comme déjà évoquées, les amendes pourront atteindre 250'000 francs si les actions sont commises intentionnellement.

Diverses mesures sont de plus introduites dans le Code pénal. Une action pénale pourra notamment être décrétée sur 5 ans.

1.4. LIPDA

La Loi valaisanne sur l'Information du public, de la Protection des Données et de l'Archivage (LIPDA) du 9 octobre 2009 est la seule loi actuelle pour le canton du Valais. Elle regroupe des dispositions relatives à l'information du public et l'accès aux documents officiels (transparence), la protection des données personnelles ainsi que l'archivage des documents officiels. (Canton du Valais, s.d.) Bien qu'elle ne soit pas décrite en détail dans ce document, il est important de signaler son existence étant donné que la HES-SO Valais siège dans le Canton du Valais.

Figure 2 : Illustration LIPDA

Source : (Canton du Valais, s.d.)

La majorité des articles de cette loi cantonale rejoignent la loi fédérale (LPD). Cependant, elle est plus exhaustive et peut différer sur certains points. Les catégories des autorités soumises au champ d'application sont définies plus précisément et le délai pour un droit d'accès à des données personnelles est fixé à 10 jours.

Enfin, une personne doit être informée d'éléments spécifiques lors de la collecte de ses données (identité du maître du fichier, finalité du traitement, catégorie(s) de destinataires s'il y a communication, droit d'accès aux données, ainsi que les conséquences liées au refus de fournir les données personnelles demandées).

1.5. Synthèse légale

L'Europe a très clairement de l'avance par rapport à la Suisse avec son règlement en matière de protection des données. De plus, la RGPD est beaucoup plus précise en termes de traitement de données et de sanctions que la LPD effective.

Les principes restent très similaires dans la forme : licéité, loyauté, transparence, finalité, proportionnalité (minimisation), exactitude, limitation de la conservation, intégrité et confidentialité (sécurité). La définition des données dites « protégées » (personnelles ou sensibles) est identique à l'exception de la biométrique et la génétique qui sont déjà considérées comme des données sensibles dans la partie européenne alors que la LPD effective ne les prend pas en compte.

Des écarts existent au niveau des chiffres. Le fait de devoir tenir un registre des traitements sera nécessaire pour les entreprises suisses de plus de 50 collaborateurs contre 250 collaborateurs pour les entreprises européennes. Aussi, les amendes sont beaucoup plus élevées avec la RGPD (4% du chiffre d'affaires ou 20 millions d'Euros) que le projet de LPD (250'000 francs).

La LPD actuellement appliquée date de 1992, soit au tout début de l'ère d'internet. L'évolution technologique a été considérable jusqu'à nos jours. Malgré les révisions logiques de certains éléments, cette loi reste donc assez vétuste et son projet de révision ambitionne donc une loi revue de fond en comble.

Figure 3 : Informations à donner lors de la collecte de données

	RGPD - Données obtenues directement auprès des individus	Projet LPD
Identité du responsable du traitement ou du représentant légal et du DPO le cas échéant	✓	✓ (sans DPO)
Les finalités du traitement, leurs bases légales et l'intérêt légitime poursuivi par le responsable de traitement (si le traitement est fondé sur cette base légale)	✓	Finalités uniquement
Les destinataires/catégories de destinataires	✓	✓
La liste des droits des individus	✓	X
Le droit de déposer une plainte devant l'autorité de protection des données compétente	✓	X
L'éventuel transfert des données à l'étranger et les garanties mises en place	✓	✓
La durée de conservation des données ou les criètres utilisés pour calculer cette période	✓	X
Mention du droit pour l'individu de retirer son consentement à tout moment	✓	X
Si la fourniture des informations est requise (i) par la loi ou (ii) une obligation contractuelle et les conséquences en cas de refus	✓	X
L'existence de décisions automatiques, les critères de décision, leur importance et les conséquences associées	✓	Existence de décisions automatisées + droit d'être entendu

Source : (Pintado, 2017)

Ainsi, le projet de révision de la LPD et la RGPD, malgré leurs différences, ont un but identique, à savoir la protection d'une personne physique. Leur avenir est indéniablement commun et il est très probable que les différentes notions définies dans les textes de loi s'uniformisent entre l'Europe et la Suisse.

De plus, l'adaptation suisse au droit européen est nécessaire pour que la Commission européenne reconnaisse la Suisse comme État tiers offrant un niveau de protection des données adéquat. C'est la condition pour que les échanges de données transfrontières restent possibles, chose extrêmement importante pour l'économie suisse.

1.5.1. Enjeux des entreprises suisses

Comme le champ d'application de la RGPD est très large, les entreprises suisses ont de fortes chances d'y être soumises. Il est donc nécessaire d'acquérir une certaine compétence en matière de protection des données personnelles et de définir ses responsabilités à l'interne.

Les entreprises suisses ont donc un double avantage de suivre la RGPD étant donné que la consultation de l'avant-projet de la nouvelle loi fédérale LPD s'est achevée.

La tâche s'annonce néanmoins ardue pour ce qui est « probablement le changement le plus important des règles sur la protection de la vie privée depuis deux décennies ». (Garessus, 2017)

1.5.2. Procédures de mises en conformité

Trois aspects importants sont à prendre en compte pour s'assurer d'être en conformité avec ces textes. (Labate, 2018)

Le premier concerne la partie juridique. Il est important de pouvoir être conseillé à l'externe sur le traitement des données ou de posséder un DPO dans l'organigramme de l'entreprise. Ainsi, diverses formations sont possibles et très en vogue avec l'actualité (séminaires, formation de responsable de la protection des données en entreprise, etc.) si l'engagement d'une nouvelle personne n'est pas souhaité.

Le deuxième aspect est en rapport avec la partie technique. Il faut adapter son infrastructure pour qu'elle soit parfaitement conforme. Cela concerne principalement le développement de solutions techniques et la sécurité de l'entreprise.

Enfin, toute l'organisation doit être revue. Un rôle « officiel » doit être défini pour la personne responsable du traitement des données. Les entreprises doivent modifier leur politique de confidentialité et certains contrats en cours pourraient être reformulés. Un mandat peut cependant être délivré à l'externe pour cette tâche.

Afin de s'assurer à toutes les contraintes, il est utile de viser une conformité à la loi européenne au lieu de se baser sur le projet de révision suisse en cours. L'important est, dans un premier temps, de pouvoir montrer que les risques ont été compris et que des démarches correctrices sont en cours. Comme déjà évoquée, une mise à jour purement informatique ne suffit pas, il faut effectuer une démarche transversale, qui va devoir faire travailler ensemble l'informatique, le marketing, le commercial, les RH. C'est donc un véritable enjeu stratégique. (Frammery, 2018)

Dans cette démarche, la CNIL définit 6 étapes claires (CNIL, s.d.) :

1. Désigner un pilote : nommer un « chef d'orchestre » qui exerce une mission d'information, de conseil et de contrôle en interne.
2. Cartographier : recenser de façon précise les traitements de données personnelles.
3. Prioriser : identifiez les actions à mener pour se conformer aux obligations actuelles et à venir selon les risques.
4. Gérer les risques : si des risques sont identifiés, il faut mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données (AIPD).
5. Organiser : mettre en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment.

6. Documenter : pour prouver sa conformité au règlement, il est nécessaire de constituer et regrouper toute la documentation.

Afin de faciliter ces étapes, divers outils existent sur le marché et seront ainsi présentés dans ce document.

1.6. Situation de la HES-SO

Dans le but de se mettre en conformité avec ces deux lois, la HES-SO évalue actuellement ses risques en interne. En effet, les conséquences pourraient être nombreuses pour la HES-SO en matière de données de recherche, de données de formation et de données administratives.

Un préavis a été donné dans un premier temps par le Rectorat, le 12 décembre 2017. (HES-SO, 2017) Par la suite, le Conseil de domaine « Économie et service » s'est réuni afin d'évoquer la situation actuelle et de déterminer un calendrier dans ce sens. (HES-SO, 2018)

Figure 4 : Logo HES-SO Valais-Wallis

Source: (HES-SO Valais-Wallis, 2017)

1.6.1. Préavis du Rectorat

Question à résoudre

La HES-SO est une institution publique qui dépose des projets européens et se retrouve directement impactée par la nouvelle RGPD. La nomination d'un DPO devient donc une mesure incontournable afin qu'il contrôle la mise en œuvre du RGPD et fasse un travail de sensibilisation interne. De plus, le DPO sera le partenaire contractuel pour les projets européens de la HES-SO.

Démarches réalisées

Pour se conformer à l'application de la RGPD fin mai 2018 et afin de résoudre cette question primordiale, la HES-SO a donc effectué certaines démarches.

Un contact informel a dans un premier temps été établi entre le Rectorat de la HES-SO et le Conseil de Rectorat *Azur+* (universités de Genève, Vaud, Neuchâtel et Fribourg). En effet, le triangle *Azur* envisage de conclure un contrat de prestations avec une Sàrl émanant d'une étude d'avocats spécialisée pour la fonction de DPO.

Une offre de la HES-SO est ainsi en cours d'élaboration, mais elle couvrirait 2 aspects :

1. Un « Kit » contenant tous les documents nécessaires pour les dépôts de projets européens
2. Un recueil des prestations en fonction des besoins de chaque institution

Cette collaboration, qui concernerait uniquement l'application au RGPD, offrirait des avantages multiples comme la mutualisation des ressources, des économies d'échelle, un échange de bonnes pratiques et un retour d'expériences.

Un diagnostic de la situation au sein de la HES-SO a également eu lieu, dans le but de pouvoir définir ensuite un plan d'action. Un groupe interdisciplinaire « protection des données » a été créé. Il est composé de :

- La responsable de l'Unité juridique du Rectorat
- Un(e) représentant(e) du Dicastère Recherche et Innovation
- Un(e) représentant(e) du Service des systèmes d'information
- La responsable de l'Unité d'aide au pilotage, Dicastère Qualité
- Un(e) représentant(e) Ra&D d'une haute école
- Une-e membre d'une unité d'appui à la conduite de projets d'une haute école

Ce groupe, sous la conduite de la responsable de l'Unité juridique du Rectorat, assurera une forme de coordination et de pilotage des problématiques de la protection des données au sein de la HES-SO durant une phase transitoire.

Les responsabilités suivantes seront couvertes par ce groupe :

- Mise en œuvre des exigences au RGPD : être répondant et suivre les démarches mandatées par la Sàrl
- Diagnostic de la situation au sein de la HES-SO : proposer une démarche permettant d'établir un diagnostic et d'envisager un plan d'action et d'amélioration ; piloter les aspects du mandat de diagnostic, répondre aux questions du mandataire et exprimer les besoins de la HES-SO
- Coordination des demandes : coordonner les travaux, au sein de la HES-SO, pour répondre à des questions ou à des demandes éventuelles de conseils en lien avec la protection des données

Selon les conclusions de ce groupe, un plan définitif sera finalement mis en place.

1.6.2. Décision du Conseil de domaine « Économie et Services »

Afin de donner suite au préavis du Rectorat, le Conseil de domaine « Économie et Services » s'est réuni dans un premier temps et a analysé finement la portée et les principaux points pertinents pour la RGPD. Des mesures concrètes ont été prises.

Un Data Protection Officer (DPO) externe d'une société à approche pluridisciplinaire et également mandatée par le Triangle *Azur+* a été donc mandaté par la HES-SO. Sa fonction principale sera d'accompagner les projets de l'UE pour ce qui concerne la protection des données.

Dans un deuxième temps, la révision totale de la LPD et ses objectifs principaux ont été évoqués. Afin d'assurer la mise en œuvre de mesures techniques et organisationnelles de protection des données au sein de la HES-SO pour un périmètre suisse, et plus précisément cantonal, un groupe interdisciplinaire de 6 personnes sera instauré. Il aura pour objectifs de proposer un mandat de diagnostic et un plan d'action en vue d'un dispositif pérenne en matière de protection des données, coordonner les demandes en matière de protection des données et fera le lien avec les démarches entreprises par le DPO.

1.6.3. HES-SO Valais-Wallis

La direction de la HES-SO Valais-Wallis devrait vraisemblablement emboîter le pas à la direction suisse. Cependant, certaines mesures ont déjà été actées comme la nomination prochaine de M. Franco Lorenzetti en tant que Data Protection Officer. Il sera soutenu dans sa prise de fonction par Mme Natacha Albrecht qui se chargera des tâches juridiques.

Dans ce sens, Monsieur Romain Schwery a récemment été nommé nouveau responsable du service informatique et de la sécurité des systèmes d'information de la HES-SO Valais. Son rôle sera, de ce fait, également décisif dans les prises de décisions et enjeux futurs concernant la protection des données au sein de la HES-SO Valais.

1.6.4. Instituts

Les instituts qui se rattachent à la recherche au développement pour la HES-SO Valais-Wallis font face à beaucoup d'inconnus. Deux collaborateurs de différents instituts ont été sollicités.

Il y aurait globalement beaucoup d'incertitudes et de méconnaissances concernant ces évolutions légales à l'institut d'Informatique de Gestion (IIG). (Cotting, 2018) La majorité des chercheurs ne connaitraient pas précisément les aspects légaux et les projets existants ne sont, de ce fait, pas vraiment conformes avec ces changements d'envergure ; les bases de données regroupant les données collectées sont par exemple inadaptées.

Les chercheurs ne paraissent actuellement pas préparés à ces changements de conception, car cela requiert beaucoup du temps pour assimiler les changements légaux et répondre aux demandes.

Avant de prendre des décisions concrètes sur les mesures à adopter, l'institut IIG attend une décision claire de la direction HES-SO. Néanmoins, un discours a été fait lors d'une séance d'institut. Un article sur la formation pour les développeurs et quelques cours en ligne pour se former ont ainsi été présentés et des indications sur les futurs rôles décisifs ont été précisées. L'institut préconise pour l'instant une série de bonnes pratiques et conseils à ses chercheurs afin de ne pas prendre de décisions qui pourraient aller à l'encontre de celles que prendra la direction de la HES-SO. Une sensibilisation a donc été faite et il faudra observer si cela s'appliquera dans la pratique.

Un enjeu de taille existe cependant au niveau de la recherche pour les projets européens : les partenaires de recherche en Europe pourraient penser que la HES-SO n'est pas compatible avec le RGPD et des pertes de contact et de partenariat pourraient se présenter, les chances de financement pour ces projets seraient également réduites.

Du côté de l'institut Recherche et Développement (IEM), 3 typologies de données sont principalement récoltées : des données d'entreprises, des données résultantes d'enquêtes et des données de macro/micro-économies (brutes). Des données sensibles peuvent être contenues dans les données d'entreprise, mais également dans les données économiques (santé, préférences de consommation, salaires et classes sociales par exemple).

Des enjeux majeurs concernent une possible réorganisation interne, car actuellement aucune stratégie commune pour la gestion des données n'est définie entre les professeurs, aucun registre n'a donc été mis en place. Bien que toutes ces données seraient stockées en suisse, leurs droits d'accès restent flous à ce jour.

Les données d'enquêtes sont bien sûr anonymisées lors de leur publication, mais restent stockées en « clair » au sein de l'institut. Les données relatives à la recherche devraient être en règle avec la législation, mais ce sont les données en lien avec des mandats d'entreprises diverses qui pourraient poser problème étant donné que l'institut travaille aussi directement avec les entreprises en activité annexes à la recherche pour la HES-SO Valais-Wallis. Aussi, les clauses de confidentialités ne suivent aucun standard précis bien qu'elles soient basées sur les modèles de l'EPFL de manière générale.

2. État de l'Art technique

2.1. Outils d'accompagnement aux entreprises

Afin d'accélérer la mise en conformité au RGPD et de par l'ampleur de cette loi sur les activités des entreprises, diverses solutions logicielles destinées directement aux entreprises ont été mises en place.

Divers sites et articles de presse proposent des conseils basiques à suivre. Mais, selon la taille et le domaine d'activité(s) d'une entreprise, des recommandations personnalisées pourraient être nécessaires afin de mieux cibler les besoins réels. Des outils plus adaptés utilisent ainsi plusieurs techniques présentées ci-dessous pour répondre à ces besoins. (Biseul, 2018) (Product Hunt, 2018)

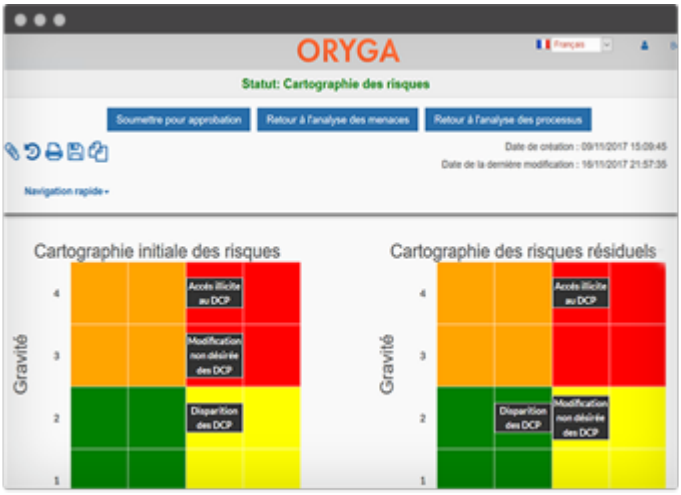
Aucun outil spécialisé pour la LPD suisse n'existe à ce jour. Cela s'explique par le fait que la loi actuelle date de 1992 et que son périmètre n'est pas adapté au traitement numérique actuelle des données. Aussi, son projet de révision est encore en discussion sur certains aspects et n'est, par conséquent, pas en vigueur.

2.1.1. Automatisation de la cartographie des traitements

Après avoir nommé un DPO dans l'entreprise, la cartographie des traitements de données personnelles est la deuxième étape recommandée par la CNIL. (CNIL, s.d.)

Un éditeur français, *BMI System*, s'est ainsi associé à *IBM* et *Ageris Group* pour réaliser la solution SaaS **ORYGA**. Cette solution va cartographier dynamiquement les traitements de données en rapport aux données personnelles dans les systèmes d'information après que les éléments requis aient été renseignés dans des champs préremplis selon la finalité, les données collectées ou les exigences réglementaires. Chaque traitement introduit est analysé pour valider sa conformité au RGPD, ce qui permet d'identifier les écarts et les actions correctives à planifier. L'impact d'un traitement sur la vie privée est ensuite évalué selon une méthode préconisée par la CNIL. Finalement, les actions liées aux droits des personnes concernées sont documentées dans différents registres afin de démontrer sa conformité. (ORYGA, 2018)

Figure 5 : Analyse d'impact ORYGA



Source : (ORYGA, 2018)

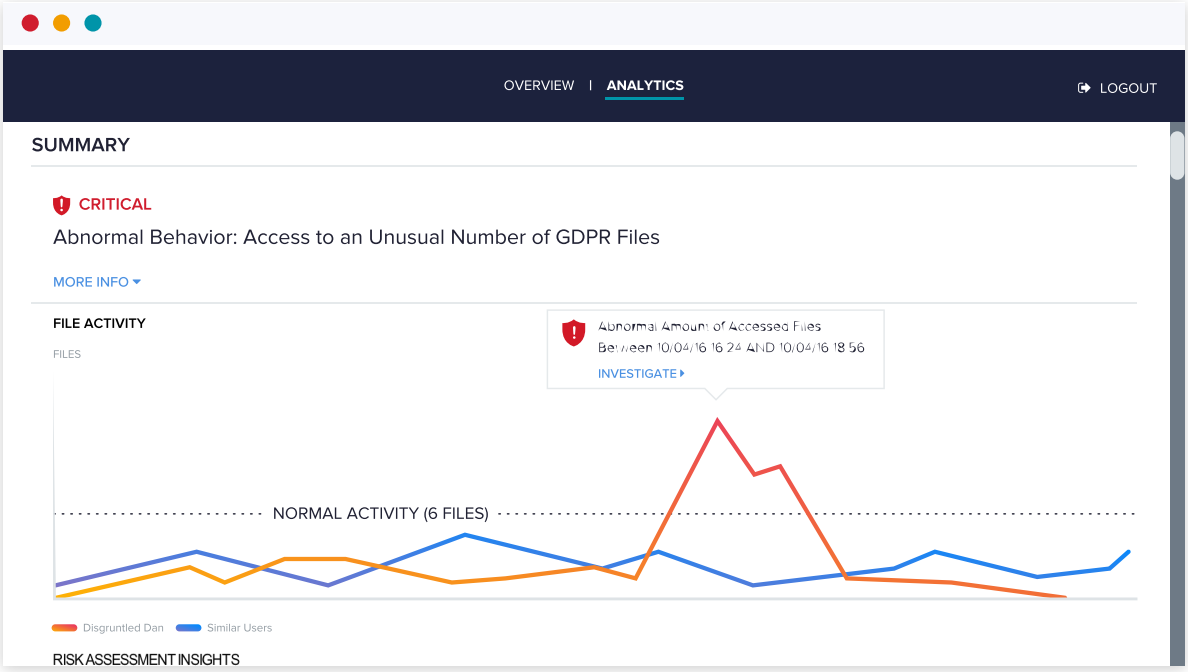
2.1.2. Identification des données sensibles

Identifier les données, contenant des informations personnelles, collectées ou gérées par une entreprise peut se révéler difficile selon le volume de données en sa possession.

Varonis, une firme experte en cybersécurité, propose plus de 280 modèles exclusifs (parmi ces derniers figurent les numéros d'identification nationale, les informations d'identification des véhicules, les numéros de téléphone, les données bancaires, etc.) qui identifient et classent les données soumises au GDPR des 28 pays de l'UE. Ce logiciel, **GDPR Patterns**, aide à découvrir, gérer et protéger les données visées par le règlement européen.

Une fois les modèles nécessaires identifiés, les entreprises sont en mesure de produire des rapports sur les données concernées par le RGPD : droits, accès ouverts et données obsolètes. Ces modèles et classifications aident à répondre directement aux exigences du RGPD, en mettant en place des politiques de sécurité pour surveiller les données visées par le règlement et émettre des alertes à l'interne. (Varonis, 2018)

Figure 6 : Analyse avancée de sécurité avec GDPR Pattern



Source : (Varonis, 2018)

2.1.3. Analyse d'impact

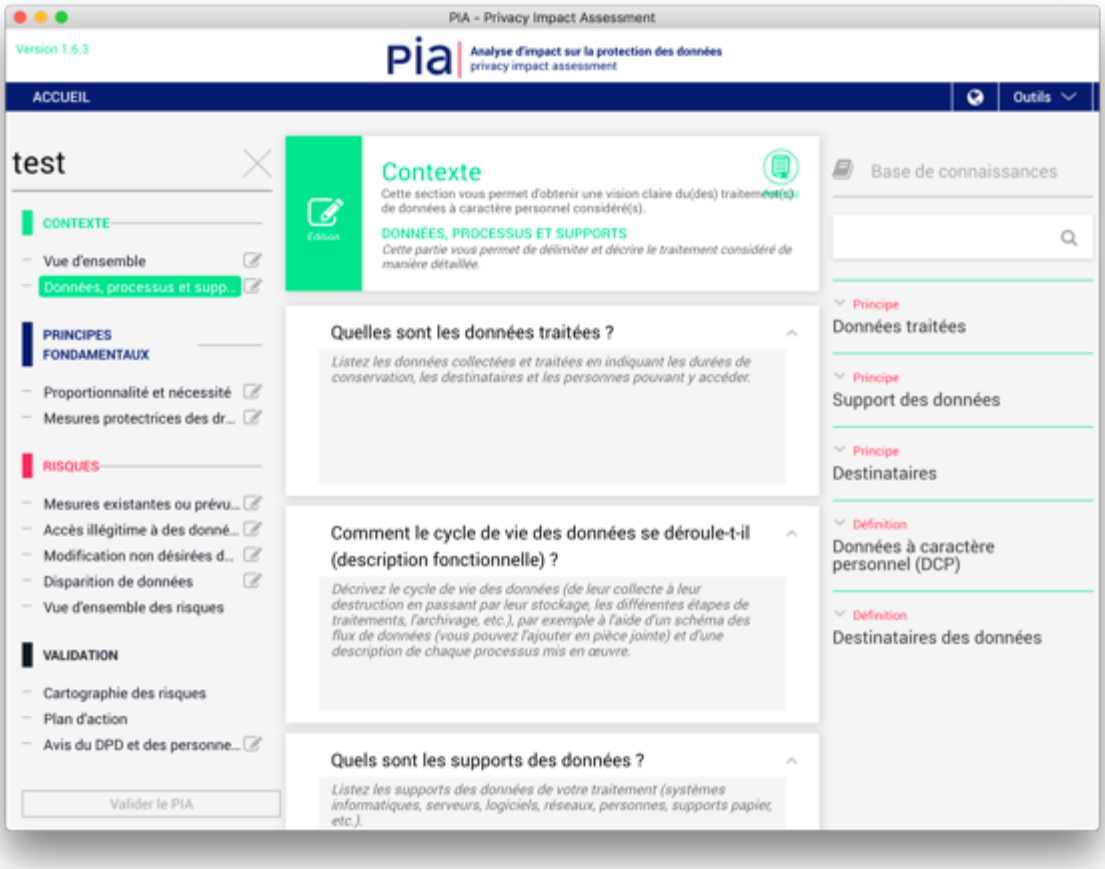
Dans l'univers numérique, la CNIL est le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits. (CNIL, 2018)

Cette autorité administrative indépendante a développé son propre outil pour conduire une analyse d'impact sur la protection des données. Ce logiciel, **PIA**, est libre (*open source*), gratuit, multiplateforme (disponible sur Windows, macOS et Linux) et disponible en plusieurs langues.

Il s'inscrit dans une démarche d'accompagnement aux responsables de traitements dans la mise en œuvre des obligations du RGPD et simplifie la conduite d'une analyse d'impact relative à la protection des données. Cet outil vise aussi à faciliter l'appropriation des guides PIA de la CNIL. (CNIL, 2018)

Un PIA pourra être ajouté et évalué selon certains critères. Quatre catégories d'informations à fournir sont délimitées par ce logiciel.

Figure 7 : Interface de l'outil PIA



Source : (CNIL, 2018)

Le **contexte** se précise selon le traitement qui fait l'objet de l'étude, les responsabilités liées au traitement, les référentiels applicables, les données collectées et traitées, le cycle de vie de ces données et les supports des données.

Les **principes fondamentaux** sont introduits selon les finalités du traitement, les fondements licites du traitement, le respect de la minimisation des données, l'exactitude des données, la durée de conservation des données, l'information du traitement, la manière du consentement obtenu, le droit d'accès et de portabilité, le droit à l'oubli, le droit d'opposition, les obligations du sous-traitant et la protection des données en cas de transfert hors de l'UE.

Des mesures sont créées afin de déterminer des **risques** spécifiques selon un accès illégitime à des données, une modification non désirée de données ainsi qu'une disparition de données.

La **validation** regroupe enfin le positionnement des risques selon une cartographie et des plans d'action peuvent résulter de ce constat tout en précisant les avis du délégué à la protection des données ou des personnes concernées.

Une base de connaissance peut également être consultée tout au long de l'utilisation du logiciel.

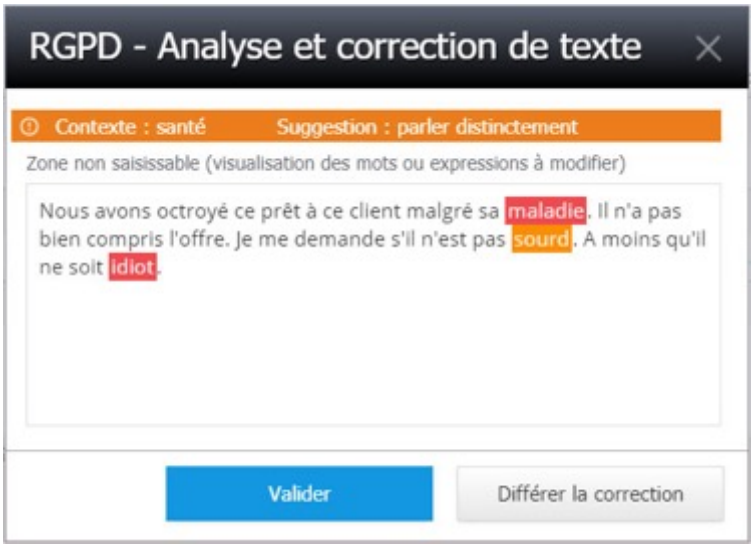
2.1.4. Détection des données prohibées

Éditeur de solutions logicielles dans les domaines du CRM, de la Data Intelligence et de la Business Analytics, *Coheris* propose une solution d'identification des données personnelles sensibles basée sur l'analyse textuelle. (Coheris, 2018)

Dans toutes les applications (CRM, ERP, RH, …), des champs type « Commentaires » ou autres peuvent être intégrés, dans lequel l'auteur saisit des informations relatives à un dossier, un client, etc. Le RGPD impose des règles strictes quant au contrôle de ces zones de risques pouvant directement concerner la vie privée des personnes.

RGPD Text-Control contrôle ainsi les espaces de textes libres de ces applications pour éviter la saisie de données dites à caractère sensible (santé, vie sexuelle, opinions politiques, etc. ou encore des commentaires subjectifs ou des jugements de valeur). Il permet également aux responsables de traitement de contrôler les zones de risques pouvant nuire à la conformité de leur entreprise à la nouvelle RGPD. (Coheris, 2018)

Figure 8 : Exemple d'utilisation de Text-Control



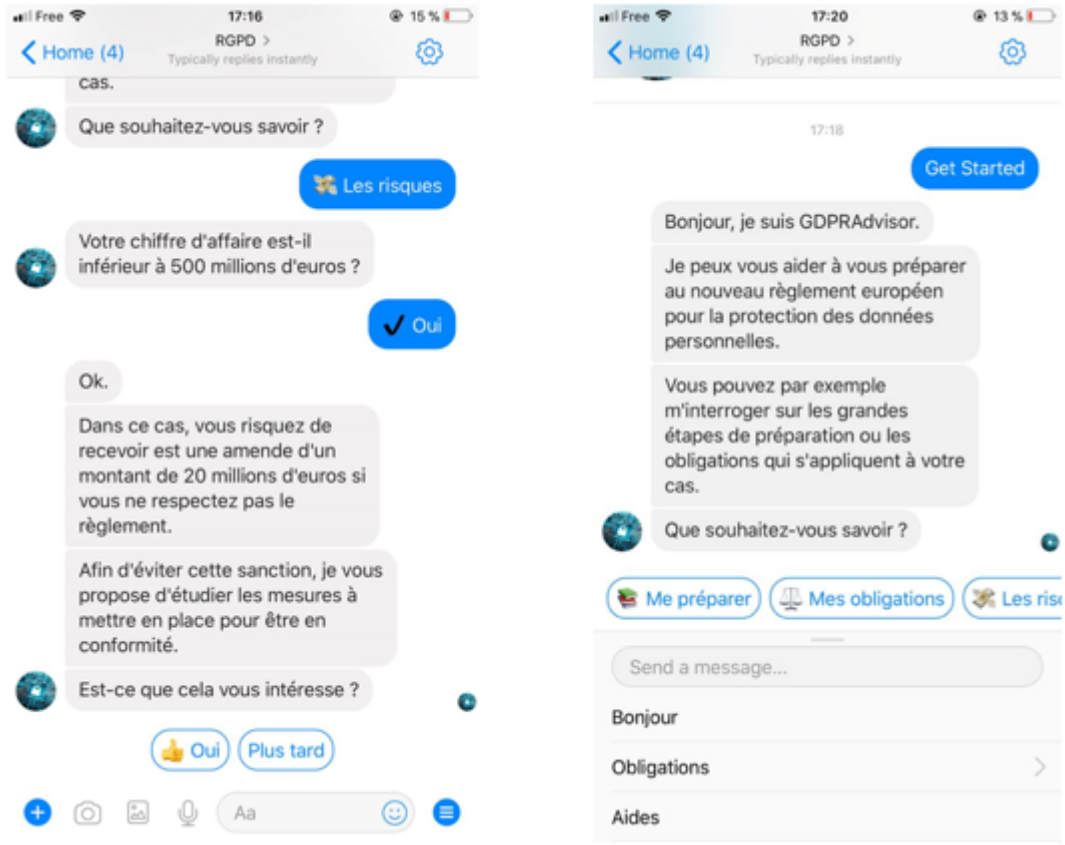
Source : (Biseul, 2018)

2.1.5. Intelligence artificielle

Le nouveau règlement ambitieux RGPD peut se révéler particulièrement dense et épineux. En effet, il peut susciter de nombreuses interrogations voire des incompréhensions ou craintes pour les entreprises selon leur taille ou leur domaine d'activité.

C'est pourquoi un cabinet français de conseil en transformation digitale, *Kynapse*, a développé un agent conversationnel (*chatbot*) utilisant la gamme de technologies d'intelligence artificielle *IBM Watson Assistant*. Il est capable d'accompagner et de conseiller les entreprises francophones en France et en Europe dans leur découverte du règlement et sa mise en œuvre.

Figure 9 : Exemples de dialogue avec le *chatbot* GDPRAdvisor



Source : (Kynapse, 2018)

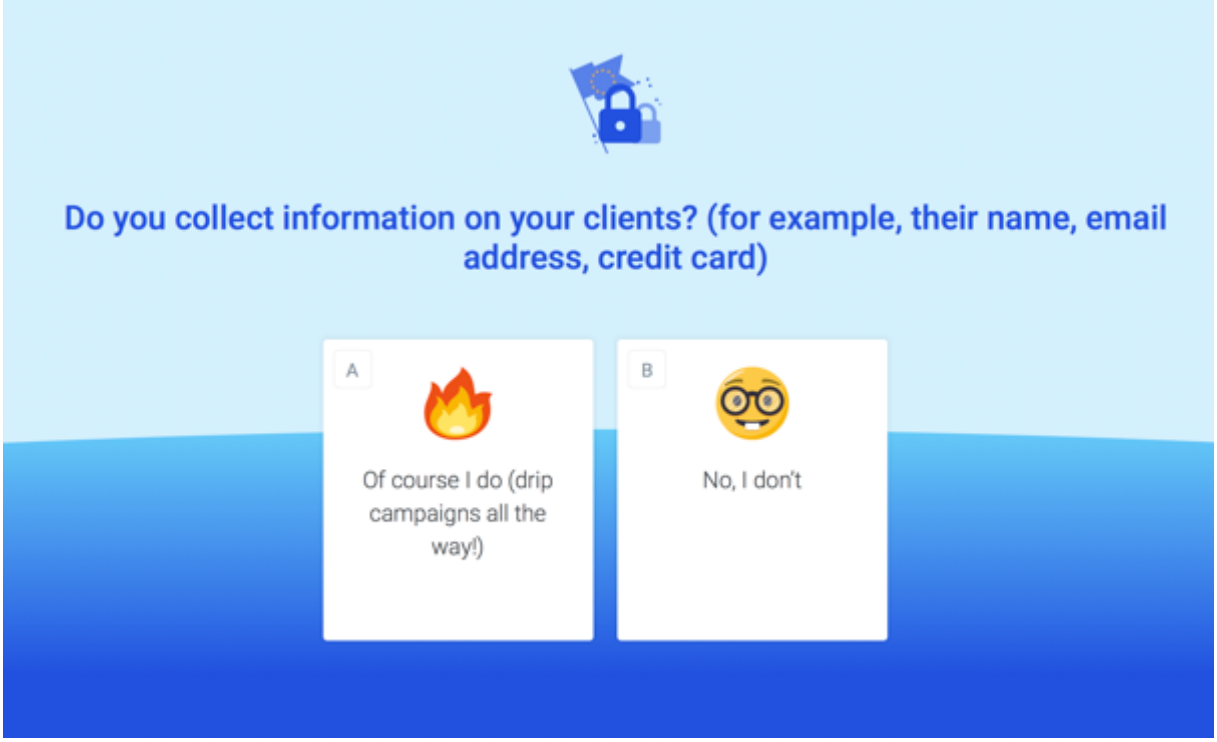
GDPRAdvisor, disponible sur la plateforme *Facebook Messenger*, propose à l'utilisateur d'évaluer sa situation à l'aide de plusieurs questions qui lui permettent de déterminer s'il est dans l'obligation d'établir un registre de traitement, de réaliser une analyse d'impact, de désigner un DPO ou encore de réorganiser ses processus de transferts de données. Son objectif vise à obtenir une liste des grandes étapes à suivre pour se mettre en conformité et être redirigé vers des contenus pertinents fournis, par exemple, par la CNIL. (Kynapse, 2018)

2.1.6. Questionnaires et listes de vérification

Des questionnaires en ligne sont également disponibles afin d'aider les entreprises dans les démarches à entreprendre.

Mailjet, une entreprise de création automatique d'e-mails, a développé un site web qui propose un quizz pour les entreprises utilisant ses services sous forme de cases à sélectionner qui peut être rempli rapidement. **The Ultimate GDPR Quiz** permet ainsi d'évaluer avec un score selon une échelle de 1 à 10 si une entreprise est conforme aux principes du RGPD (le domaine d'activité, le nombre d'employés, les services offerts dans l'UE, le type de données collectées, la sécurité des données stockées, la minimisation, le consentement libre, la politique de confidentialité, etc.). (Mailjet, 2018)

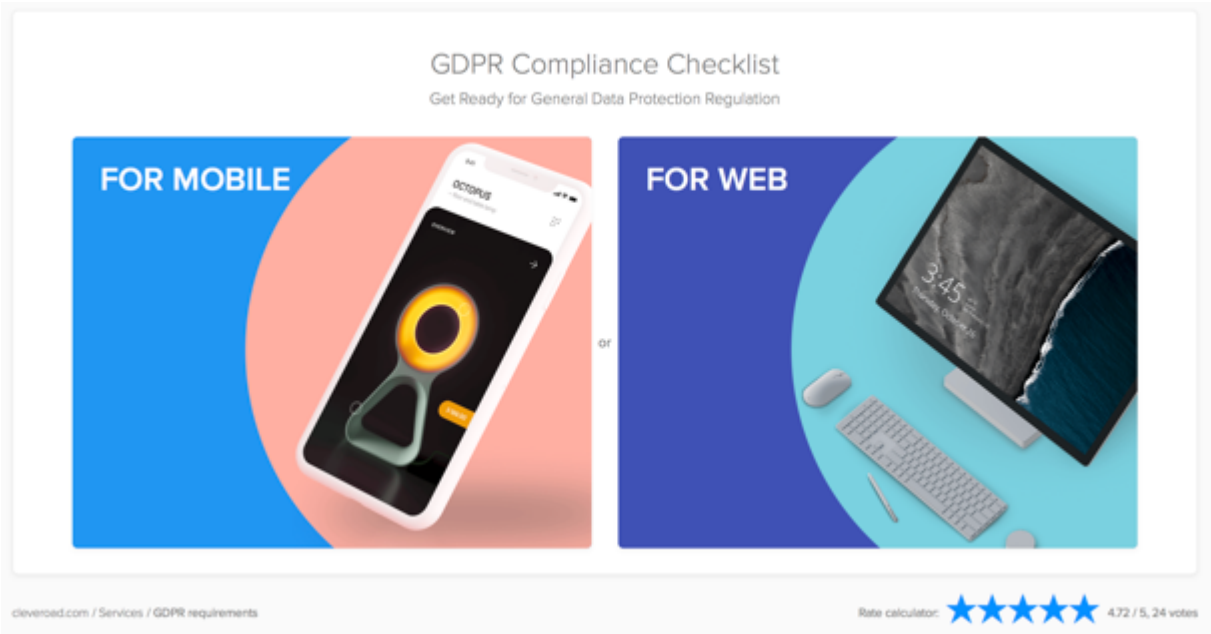
Figure 10 : Exemple de question de The Ultimate GDPR Quiz



Sources : (Mailjet, 2018)

Dans le même ordre d'idée, *Cleveroad*, une entreprise de développement web et mobile a conçu un outil similaire qui va lister une liste de tâches à effectuer pour s'assurer de suivre la RGPD. Cet outil est destiné plus précisément aux entreprises qui offrent des services à travers un site web ou une application mobile. Avec **GDPR Compliance Checklist** une entreprise va ainsi remplir un questionnaire en 10 étapes se rapportant à son site web ou son application mobile et obtenir une liste des fonctionnalités à implémenter pour assurer la conformité de ses services. (Cleveroad, 2018)

Figure 11 : Utilisation de GDPR Compliance Checklist



Source : (Cleveroad, 2018)

2.2. Data Protection Officier

Comme déjà évoqué, avec le RGPD et le projet de révision de la LPD, la nomination d'un DPO peut se révéler obligatoire sous certaines conditions, notamment dans les institutions publiques et les entreprises qui traitent des données à grande échelle. Certes cette nomination ne reste pas toujours obligatoire, mais son apport est fortement conseillé. Son rôle sera une aide bienvenue dans le maintien de la conformité pour une entreprise dans la durée.

Un DPO est capable de coordonner les actions à effectuer dans les différents services d'une entreprise en l'aidant à atteindre ses objectifs tout en restant conforme avec la réglementation.

Figure 12 : 8 bonnes pratiques pour être un bon DPO

Source : (Fockens, 2018)

Son rôle est complexe dans la structure d'une entreprise. Outre d'excellentes connaissances en informatique et en cybersécurité, il doit posséder une bonne culture juridique, particulièrement en droit des nouvelles technologies. Enfin, il doit pouvoir bien communiquer avec les différents responsables de services et les sensibiliser en permanence. (CNIL, 2018)

2.2.1. Formations

Diverses formations de DPO existent pour les entreprises qui souhaiteraient, par exemple, former un employé déjà présent dans l'entreprise.

Le **Centre Universitaire d'Informatique de l'Université de Genève** (CUI Unige) a organisé des séminaires, sur 7 jours, pour un « Responsable de la protection des données en entreprise / DPO ». Ils se déroulent en deux modules (introduction et approfondissement), un master class et des examens. Les séminaires ont l'avantage de proposer une approche pluridisciplinaire de la mise en œuvre de la protection des données en entreprise. Des intervenants de marque sont également présents, dont le préposé fédéral suppléant à la protection des données et à la transparence.(CUI Unige, 2018)

Dans un registre plus technique, l'**Association internationale des professionnels de la protection de la vie privée** (IAPP), la première organisation internationale des professionnels de la protection des données, fournit des ressources utiles aux délégués à la protection des données pour les clients, salariés, partenaires, fournisseurs et sous-traitants. Elle offre des formations en ligne pour les professionnels qui traitent de ressources et connaissances spécifiques à leur secteur d'activité.

Elle propose également des certifications « Professionnel certifié de la confidentialité de l'information » adaptées selon le secteur géographique (Asie, Canada, Europe et secteur privé américain). En complément, du contenu en ligne est présenté (des publications en ligne, des blogs, des livres, des rapports spécialisés, des podcasts et des conférences Web) et des conférences se déroulent 6 fois par an à travers le monde. (IAPP, 2018)

Figure 13 : Programmes de certifications IAPP

Source : (IAPP, 2018)

Enfin, la Filière Informatique de Gestion de la HES-SO Valais propose, depuis peu, une formation continue « ADAPTER SON ENTREPRISE AU RGPD ». Cette formation, destinée aux chefs d'entreprises ou indépendants, utilisateurs des systèmes d'information et responsables de services, a comme objectifs de :

- Comprendre les exigences du règlement général sur la protection des données (RGPD)
- Cerner quels aspects de la société impliquée sont concernés par le RGPD
- Établir des mesures concrètes pour se mettre en conformité

Les avantages de cette formation sont sa durée relativement courte (2 demi-journées) et son prix très accessible (200 francs). (HES-SO Valais-Wallis, 2018)

2.2.2. Externalisation du DPO

Toutes les entreprises ne pourront pas se permettre de former ou d'engager un DPO selon leur volume de données traitées et leur taille. Certaines choisiront donc d'externaliser le rôle de DPO. Ce choix peut apporter divers avantages comme une indépendance vis-à-vis de l'entreprise, une absence de conflit d'intérêts, des coûts plus raisonnables, une disponibilité directe sans formation préalable, une expertise assurée avec des renforts possibles (juristes ou avocats) si nécessaire ainsi qu'un remplacement de DPO facilité par une relation uniquement contractuelle.

Conformément à ces atouts, l'entreprise suisse **Data Protection Company** propose ainsi d'externaliser le rôle de DPO et offre un support supplémentaire grâce à ses équipes certifiées. (Data Protection Company, 2018)

Figure 14 : Services proposés par Data Protection Company

Source : (Data Protection Company, 2018)

2.3. Synthèse des outils

Les différentes approches choisies dans le fonctionnement de ces différents outils prouvent que la RGPD est relativement « jeune » et que le marché des outils d'accompagnement aux entreprises et encore relativement vaste. Le besoin réel de ce genre d'outils par les entreprises ne semble pas précisément défini.

Certaines sociétés ont opté pour des solutions plus « classiques » comme des questionnaires à remplir manuellement en supposant que l'entreprise a déjà connaissance de tous les éléments importants pour sa conformité et pourra donc les insérer.

D'autres éditeurs d'outils préconisent une approche bien plus « moderne » et automatisée. Les outils de cartographie et de contrôle de textes permettent ainsi d'apporter directement des éléments de réponses de manière instantanée en allant directement les « piocher » dans les systèmes d'information de l'entreprise.

Les nouvelles tendances technologiques pourraient également jouer un rôle décisif dans ces procédures de mise en conformité comme le prouve l'agent conversationnel de *Kynapse*. Ce procédé visant à simuler une intelligence humaine par des machines est relativement en vogue actuellement dans l'industrie *high-tech* et très prisé par les grands groupes informatiques qui s'en servent dans le but d'améliorer la réactivité de leurs services.

Enfin, le choix de former un DPO à l'interne, d'en engager un ou de l'externaliser résultera de la taille et des activités et services offerts par l'entreprise. Cela déprendra du temps à disposition avant le début de sa tâche, le volume de travail à effectuer ainsi que la puissance financière disponible étant donné les coûts généralement élevés des formations. Cette décision sera donc propre à chaque modèle de fonctionnement d'entreprise.

3. Analyse et choix

3.1. Type d'outil

L'un des objectifs principaux de ce travail de Bachelor consiste à créer un outil d'aide à la décision qui facilitera la mise en conformité légale aux textes suisse et européen dans le cadre de la HES-SO Valais, principalement dans le contexte des Instituts de « Recherche et Développement ».

Cet outil décisionnel se présente sous forme d'un tableau de bord (*Dashboard*) contenant une série de questions et choix à sélectionner. Son but est de soutenir le DPO dans les mesures à mettre en place pour assurer une gestion adéquate des données selon leur utilisation et leur contexte au sein de la HES-SO Valais.

Étant donné qu'aucune analyse précise n'a été réalisée en interne par les instituts, une complexité existe à ce jour concernant les choix à définir pour le DPO ainsi que le résultat précis souhaité. Cet outil se définit donc comme un prototype (*Proof of concept*) fonctionnel avec des données tests et des résultats génériques.

3.1.1. Pourquoi un site web ?

Cet outil doit être évolutif et automatisé. Pour que son utilisation puisse être à la portée du DPO, son fonctionnement doit être simple, et son utilisation intuitive. Bien qu'il ne soit qu'au stade de prototype, le fait de le présenter sous forme de site web pourrait permettre de l'intégrer facilement aux solutions déjà présentes dans les systèmes d'information des instituts de la HES-SO Valais, point non négligeable pour la recherche de technologies utilisables pour cet outil.

De plus, l'accès à cet outil est grandement simplifié : en plus de son interface adaptable sur tous les supports (*responsive*), aucun logiciel supplémentaire n'est nécessaire pour son fonctionnement. En effet, après la configuration du serveur, il est accessible au moyen de n'importe quel navigateur web.

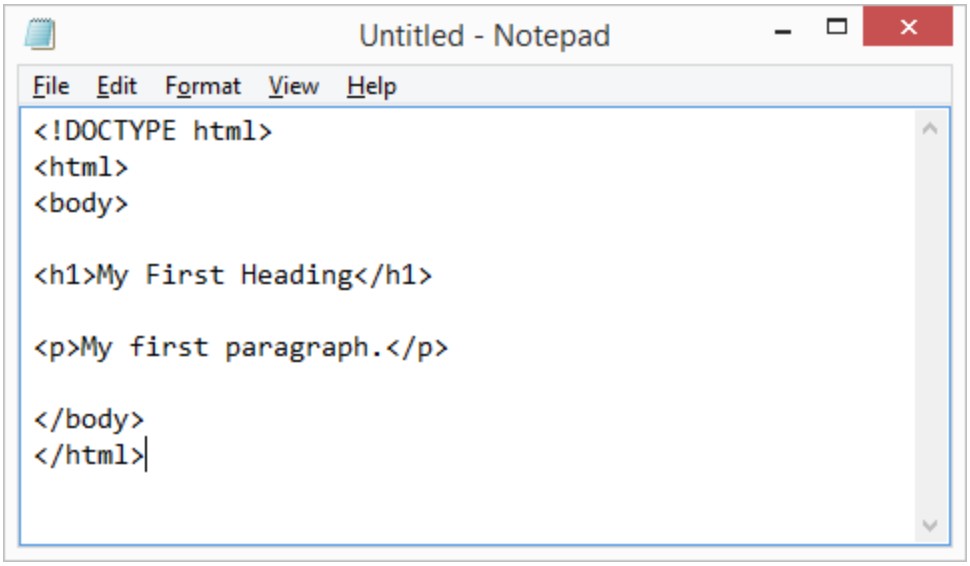
3.2. Langages de développement et Frameworks

3.2.1. HyperText Markup Language

HyperText Markup Language ou « HTML » est un langage qui se traduit en français par « langage de balises pour l'hypertexte ». Il est utilisé comme standard pour créer et afficher le contenu d'une page web. Des « additions » peuvent être couplées à ce langage pour décrire sa présentation graphique (avec CSS) et lui ajouter des fonctionnalités interactives (avec JavaScript).

Comme son nom l'indique, ce langage fonctionne grâce à un système de « balises » qui sont insérées à un texte normal. Chaque balise a une signification particulière et permet d'inclure du contenu spécifique à la page web (un titre, du texte brut, des paragraphes ou des images par exemple).

Figure 15 : Exemple de code HTML



Source : (W3Schools, s.d.)

La référence à « hypertexte » est le fait de créer des liens entre les différentes pages web et de permettre de naviguer facilement entre elles comme on le fait aujourd'hui couramment à travers n'importe quel site web.

Avec ce langage, chacun a donc la possibilité de créer et façonner des sites web. (Mozilla, 2018)

3.2.2. Cascading Style Sheets

Cascading Style Sheets ou « CSS » est un langage utilisé en complément du HTML. Également utilisé comme standard dans le développement web, il permet de décrire la présentation, notamment graphique, d'une page web.

Il décrit ainsi de quelle manière les éléments doivent être affichés (disposition des textes et médias par exemple). (Mozilla, 2018)

3.2.3. JavaScript

JavaScript ou « JS » est un langage de scripts conçu par *Netscape* et utilisé au travers de millions de pages web dans le monde entier. Il est orienté objet et très facile à assimiler. (Mozilla, 2018)

Ce langage a la particularité de s'exécuter directement sur l'ordinateur du client, c'est donc l'ordinateur de l'utilisateur qui va « recevoir » ce code et le lancer dans le navigateur web. JavaScript est alors utile pour des petites animations et interactions sur une page sans qu'on ait besoin de la recharger en permanence. (InfoWebMaster, 2018)

Figure 16 : Rôle du JavaScript avec HTML et CSS

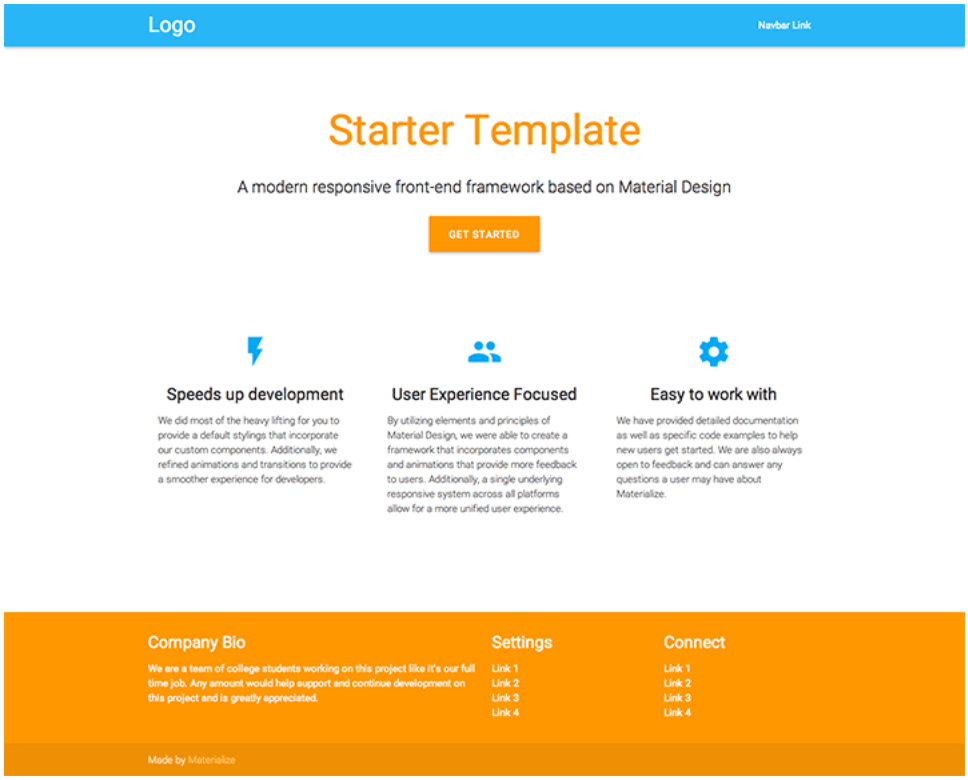
Source : (Arya, 2017)

Une bibliothèque nommée « jQuery » sera utilisée afin de simplifier la manipulation de DOM (modèle de document chargé dans le navigateur), les appels d'AJAX (pratique de programmation consistant à construire des pages Web plus complexes et dynamiques) et la gestion des évènements. Elle est fréquemment utilisée par les développeurs JavaScript et fonctionne sur une multitude de navigateurs web. (Mozilla, 2018)

3.2.4. Framework Materialize

Materialize est un *Framework* moderne basé sur le concept « Material Design ». Créé et conçu par *Google*, le « Material Design » est un langage de conception qui combine les principes classiques d'un design « réussi » ainsi que l'innovation et la technologie. (Materialize, 2018)

Figure 17 : Exemple d'une page web utilisant Materialize



Source : (Materialize, 2018)

Ce *Framework* permet aux développeurs d'améliorer considérablement le CSS d'un site web en proposant des éléments graphiques préconçus et simples à implémenter.

En combinant ce *Framework* avec le langage JavaScript et la bibliothèque « jQuery », des animations cohérentes et familiales pour l'utilisateur sont visibles. La navigation sur le site web s'effectue ainsi de manière intuitive et facilite la compréhension d'utilisation pour l'utilisateur.

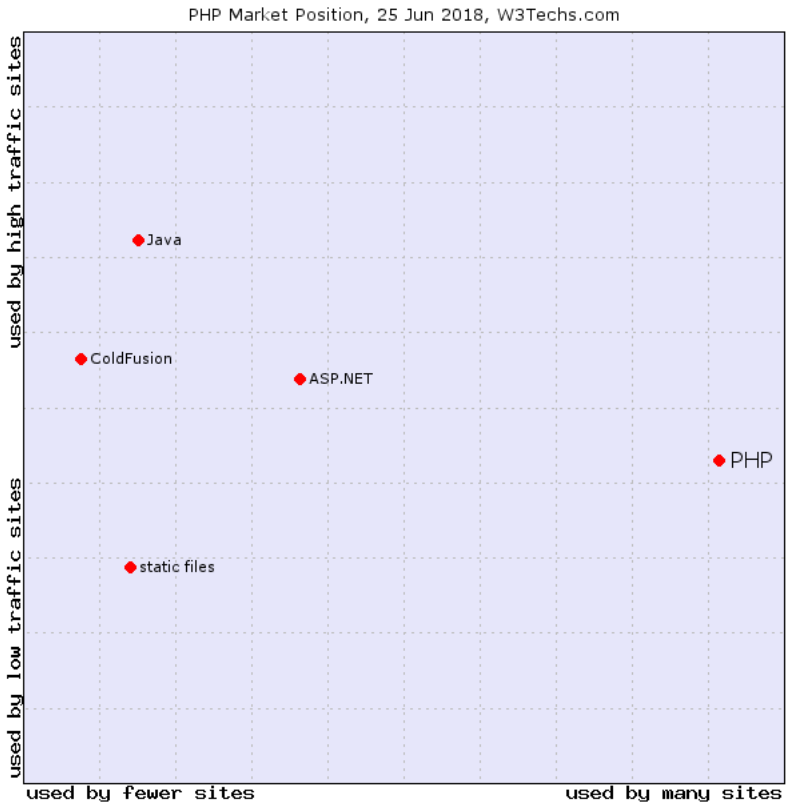
3.2.5. PHP Hypertext Preprocessor

PHP est un langage de scripts généraliste et *Open Source*. Il est énormément utilisé et a été spécifiquement conçu pour le développement d'applications web. Son intégration au HTML est ainsi facilitée. L'avantage offert par PHP est sa simplicité d'apprentissage, même pour les débutants, et son offre de fonctionnalités avancées pour les experts.

À la différence de JavaScript qui est également un langage de scripts, son code est interprété sur le serveur du site web. Son résultat sera encapsulé dans le HTML et envoyé sous cette forme au client (l'utilisateur). (The PHP Group, 2018)

En juin 2018, il a été constaté que PHP était utilisé par 83,5% des sites web, ce qui en fait le langage orienté serveur le plus populaire. (W3Techs, 2018)

Figure 18 : Position de PHP sur le marché



Source : (W3Techs, 2018)

PHP a été retenu pour plusieurs raisons évidentes dans la conception de cet outil :

- C'est un langage totalement gratuit
- Il est très performant dans son exécution
- Il est facile à apprendre et prendre en main
- Beaucoup de documentations sont disponible et sa communauté est grande
- Il gère parfaitement et nativement les requêtes d'accès aux bases de données (SQL)
- Il est très mature et sa stabilité n'est plus à prouver en étant déjà à sa septième version
- Comme il est exécuté depuis le serveur, il peut fonctionner sur tous les appareils et systèmes d'exploitation au moyen d'un navigateur web
- Il est le langage le plus standardisé par les hébergeurs web

Tableau 1 : Comparatif de langages de scriptes côté serveur avec PHP

Caractéristiques	PHP	ASP	JSP	CFML
Apprentissage	Court	Plus long que PHP	Plus long que PHP	Plus long que PHP
Hébergement web	Supporté par quasiment tous les hébergeurs	Un serveur dédié est requis	Assez supporté	Un serveur dédié est requis
Open Source	Oui	Non	Oui	Commercial et *Open Source*
Support de services web	Natif	Possible avec l'utilisation le *Framework* .NET	Possible avec des librairies à ajouter	Natif
Intégration avec HTML	Facile	Assez complexe	Assez complexe	Facile
Support de MySQL	Natif	Nécessite des pilotes supplémentaires	Nécessite des pilotes supplémentaires	La version actuelle a un support natif. Les anciennes versions utilisent ODBC
Facilement malléable avec d'autres langages	Oui	Non	Étendu en utilisant des classes et bibliothèques Java	Oui

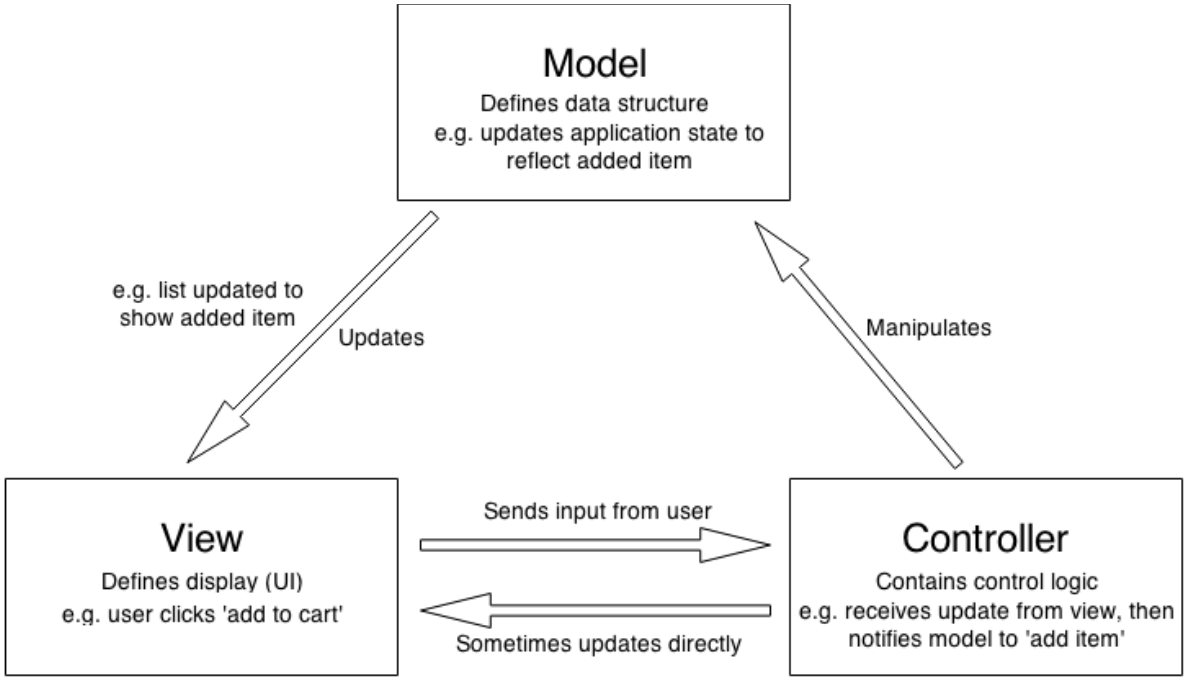
Source : (ALiveVam, 2018)

3.2.6. Model-View-Controller

MVC est un patron d'architecture logicielle populaire pour la conception d'applications web. Il est très souvent utilisé pour la réalisation d'application web avec PHP. Généralement, son utilisation permet d'implémenter des interfaces utilisateurs.

L'application est séparée en trois parts distinctes, permettant la modularité et rendant plus simple la collaboration et la réutilisation. Ce modèle rend aussi les applications plus flexibles et plus accueillantes aux itérations. (Mozilla, 2018)

Figure 19 : Schéma de structure MVC avec un exemple concret



Source : (Mozilla, 2018)

1. Le **Modèle** détermine quelles données l'application doit contenir. Si l'état de ces données change, alors le modèle va généralement avertir la vue (donc l'affichage peut être modifié au besoin) et parfois le contrôleur (dans le cas où une logique différente est nécessaire pour contrôler la modification de la vue).

2. La **Vue** détermine comment les données de l'application doivent être affichées. Cela correspond au code HTML et CSS. Son but est de montrer simplement les données issues du Modèle sans qu'elles soient modifiées ou interprétées.

3. Le **Contrôleur** fait le lien entre la Modèle et la Vue. Le contrôleur contient toute la logique de mise à jour du modèle et/ou la vue en réponse aux entrées (actions) de l'utilisateur sur l'application.

MVC est particulièrement intéressant pour notre outil, car il permet une organisation claire des différentes classes selon leur utilité.

Ainsi, notre modèle de données est contenu dans une base de données MySQL, le code de contrôle de l'application est écrit en PHP et l'interface utilisateur est écrite en utilisant HTML/CSS/JavaScript.

3.3. Infrastructure et environnement de développement

3.3.1. Serveur web local

Étant donné que l'outil est, pour l'instant, destiné à être un prototype qui nécessite encore du développement pour être opérationnel, une infrastructure locale a été mise en place, c'est-à-dire que l'outil développé est seulement accessible sur une machine physique. Une documentation pour l'installation est bien sûr disponible en annexe.

Le logiciel de serveur web **XAMPP** a de ce fait été retenu pour développer l'outil localement. Entièrement gratuit, multiplateforme et facile à utiliser et installer, cette distribution Apache contient MySQL, PHP et Perl. Elle est tout simplement l'environnement de développement PHP la plus populaire. (Apache Friends, 2018)

Figure 20 : Outils contenus dans XAMPP

Source : (ybierling, 2016)

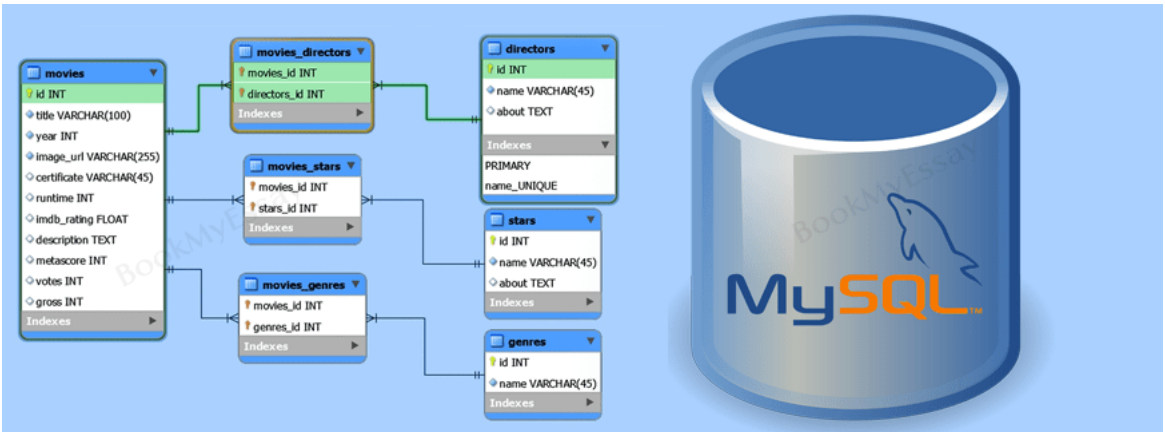
Ce paquetage *open source* simule ainsi, dans notre cas, la configuration et l'intégration d'un serveur web Apache avec PHP et MySQL, ce qui permet l'affichage et l'accès au site web.

3.3.2. Stockage des données

Afin que notre outil puisse déterminer et afficher des résultats clairs, nous allons procéder avec des données de test définies selon les cas de figure. Ces données vont devoir être stockées sur un serveur de bases de données.

Notre choix s'est porté sur **MySQL**, un serveur de bases de données relationnelles *Open Source* qui est intégré parfaitement à notre serveur web local et qui est supporté nativement par notre langage de développement. L'acronyme SQL signifie « Structured Query Language » que l'on peut traduire par « langage de requêtes structuré ». Il s'agit du langage standard pour les traitements relatifs aux bases de données.

Figure 21 : Exemple de tables et relations d'une base de données MySQL



Source : (BookMyEssay, 2018)

Ce serveur de bases de données stocke les données dans des tables séparées plutôt que de tout rassembler dans une seule table. Cela améliore la rapidité et la souplesse de l'ensemble. Les tables sont reliées par des relations définies, qui rendent possible la combinaison de données entre plusieurs tables durant une requête. (Futura-Sciences, 2018)

3.3.3. Environnement de développement intégré

Un Environnement de développement intégré (ou *IDE* en anglais) est un logiciel informatique qui permet un développement facile en lignes de code dans un certain langage. Dans notre cas, le langage principal sera le PHP et l'*IDE* va nous permettre de bénéficier de la syntaxe automatique du code avec différentes couleurs selon les mots reconnus par le moteur PHP, un alignement logique du texte ainsi que de l'autocomplétion, soit le fait de se voir proposer rapidement des bouts de code ou mots déjà préformatés lors de notre saisie.

Pour le choix de notre implémentation, deux logiciels ont été retenus : PhpStorm et Visual Studio Code. La décision de ne retenir que ces deux *IDE* disponibles sur le marché résulte du fait que divers projets personnels ont déjà été réalisés avec ces *IDE*, leur fonctionnement et utilisation sont donc familiers.

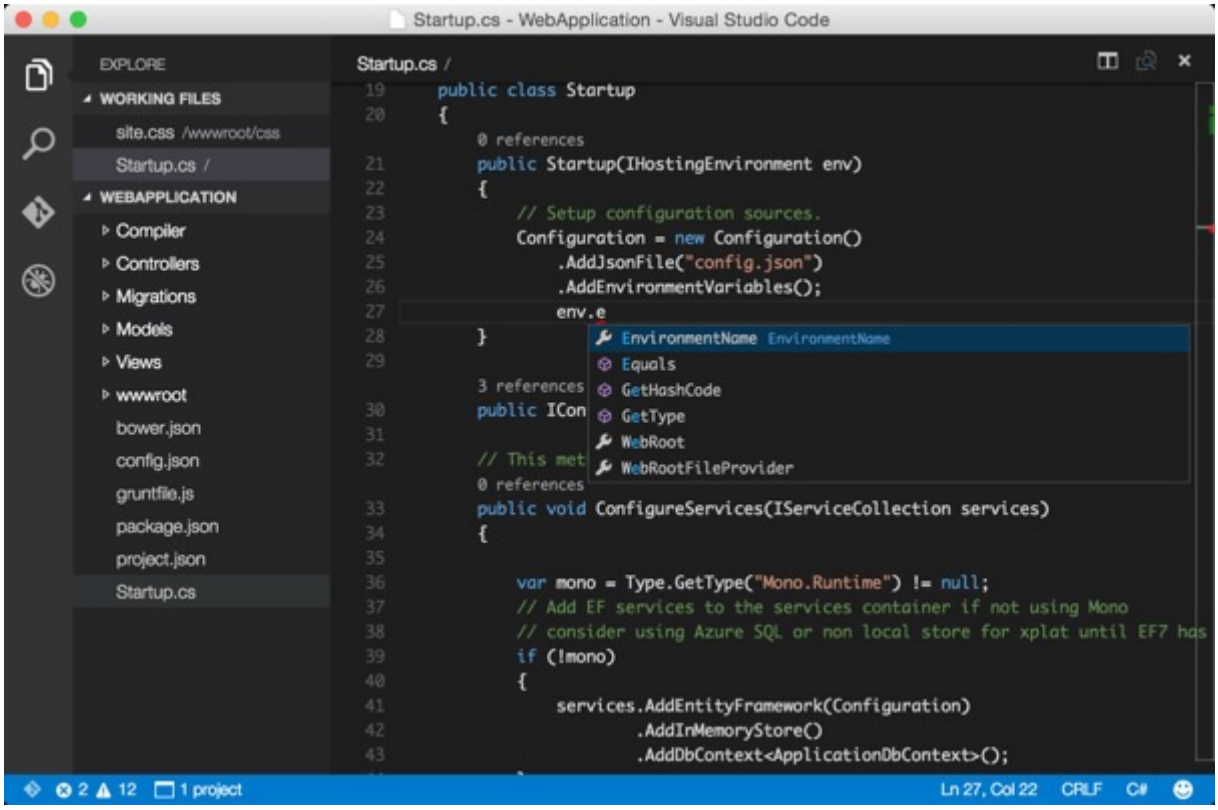
Après avoir comparé spécifiquement ces programmes, **Visual Studio Code** a été choisi comme environnement de développement intégré pour ce projet.

Les avantages pour la réalisation de notre outil sont multiples (Slant, 2018) :

- Permets le débogage PHP
- Gratuit et open-source
- Disponible sur toutes les plateformes (Windows, macOS, Linux)
- Beaucoup d'extensions sont disponibles
- Autocomplétion PHP intégrée
- Interface utilisateur moderne et intuitive
- Développement actif avec une mise à jour majeure par mois : une grande communauté l'utilise et soumet les éventuels problèmes rencontrés, ils sont ainsi rapidement corrigés

Bien qu'il soit avant tout un éditeur de code, Visual Studio Code peut, sans autre, être utilisé pour développer en PHP (Microsoft, 2018), mais aussi dans une multitude d'autres langages, sa polyvalence lui permet d'être un véritable environnement de travail destiné à tout type de développeurs grâce aux multiples extensions disponibles. Le fait qu'il soit édité par *Microsoft*, une grande entreprise informatique et « historique » dans le domaine, prouve également qu'il est un outil sérieux et performant.

Figure 22 : Interface de Visual Studio Code



Source : (alternativeTo, 2018)

En comparaison, PhpStorm est un logiciel propriétaire et payant. Une licence est nécessaire pour l'utiliser. De plus, ses fonctionnalités sont avant tout destinées à des développeurs professionnels et elles ne seraient pas toutes adaptées à nos besoins. Bien que ses principales fonctionnalités se rapprochent de Visual Studio Code, le critère du prix est donc déterminant dans notre choix.

Tableau 2 : Comparatif des IDE pour PHP

Caractéristiques	Visual Studio Code	PhpStorm
License	Libre et gratuite	Propriétaire et commerciale
Éditeur	Microsoft	JetBrains
Plateformes	Windows, macOS, Linux	Windows, macOS, Linux
Support de plusieurs langages	Oui (HTML/CSS/JavaScript inclus)	Oui (HTML/CSS/JavaScript inclus)
Avantages	Autocomplétion « IntelliSense », des centaines d'extensions disponibles, développement actif, interface moderne, terminal intégré, debugger intégré, bonnes performances	Autocomplétion intelligente, vue de la base de données, debugger inclus, interface pour GIT
Inconvénients	Autocomplétion et vérification du code pas aussi avancés, les extensions peuvent créer un bazar, limité pour un *IDE*	Logiciel propriétaire, prix élevé, consomme beaucoup de ressources, performances lentes, interface encombrée

Source : (Feed-backs de divers utilisateurs, s.d.)

3.3.4. Hébergement en ligne du code

Pour la réalisation de ce travail, un hébergement en ligne du code réalisé se révèle très utile pour la sauvegarde de l'avancée et le fait de pouvoir posséder un historique des modifications réalisées, en tout temps, afin de revenir en arrière en cas d'éventuel(s) problème(s) majeur(s). **GitLab** est le service en ligne qui a été retenu pour effectuer ces tâches. C'est un logiciel libre et gratuit qui permet également de réaliser une gestion précise de projet.

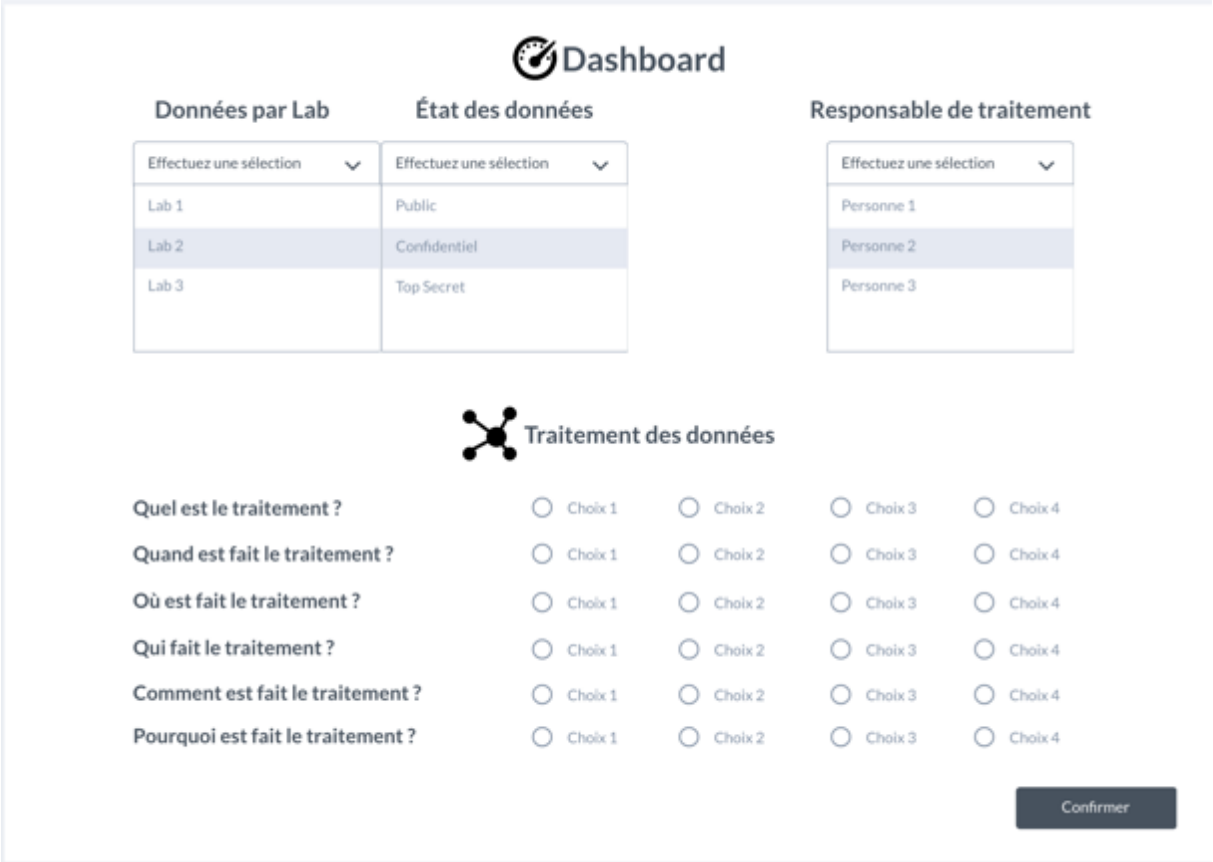
4. Développement de l'outil

4.1. Mock-ups

Afin d'avoir une idée claire et précise de la conception de l'outil à réaliser, des *mock-ups* ont été élaborés avant de débuter le processus d'implémentation. Ces réalisations purement graphiques ont ainsi permis de définir le fonctionnement de l'outil et ses vues simplement. Elles ont pu être créées avec l'outil *Marvel*[2].

En se basant sur les discussions de M. Montani avec Mme Natacha Albrecht sur les besoins de cet outil, deux vues pour l'utilisateur ont été privilégiées : une pour fournir les informations (inputs) et une autre pour afficher les résultats (outputs).

Figure 23 : Mock-up initial de la vue des inputs



Source : (Données de l'auteur, 2018)

[2] Mavel – The design platform for digital products, https://marvelapp.com

Avant de débuter le développement, la vue du questionnaire (inputs) a évolué sur certains points. Le champ « État des données » a été remplacé par « Types des données » pour mieux correspondre aux consignes légales et le choix « Responsable de traitement » a été rendu facultatif. Les questions ont aussi été revues afin d'être plus pertinentes selon les textes légaux.

Figure 24 : Mock-up de la vue des outputs

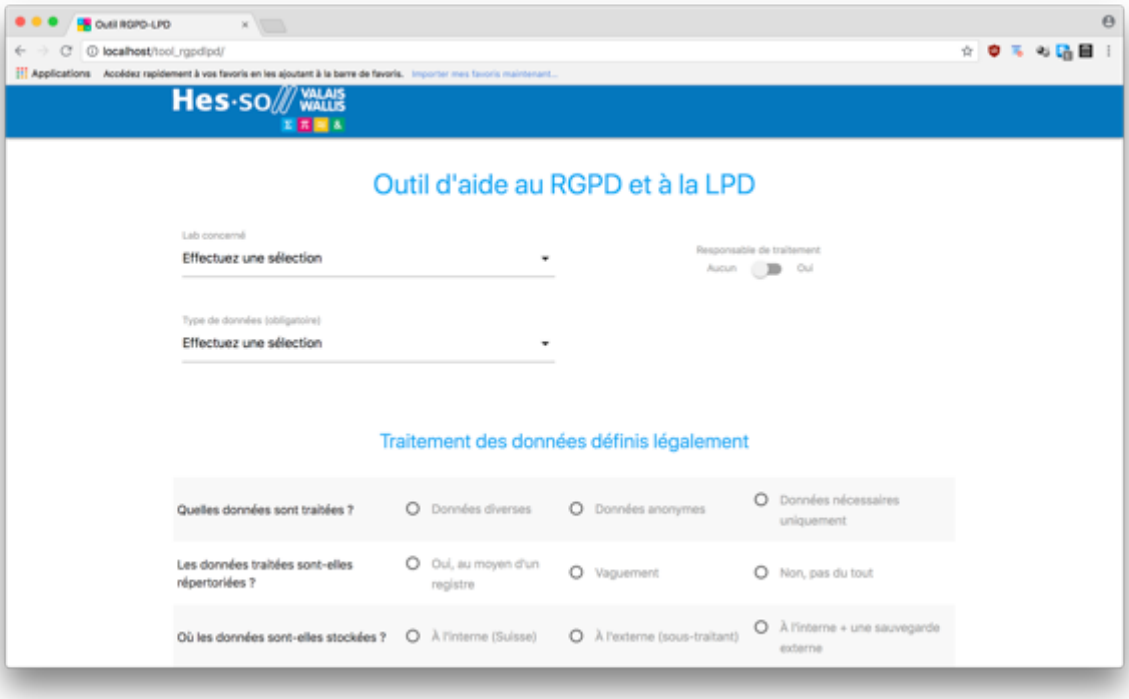
Source : (Données de l'auteur, 2018)

La vue des résultats (*outputs*) a été jugée satisfaisante et son principe conservé pour l'implémentation. Une possibilité d'afficher un récapitulatif a, dans un premier temps, été introduite afin de réaliser des tests lors de l'implémentation. Cette fonctionnalité a ensuite été estimée pertinente pour l'utilisateur et a été améliorée et maintenue.

4.2. Vue du Questionnaire (Inputs)

Pour que l'application puisse ressortir des résultats qui correspondent bien aux informations et choix fournis, cette vue permet à l'utilisateur de saisir des informations selon le cas de figure qui se présente. Elle est séparée en deux *blocs* de contenus, un pour effectuer des sélections et un deuxième avec des questions et leur réponse respective à cocher dans des cases. Un bouton « Confirmer » offre enfin la possibilité de valider le formulaire, une fois que les informations ont été insérées.

Figure 25 : Vue du Questionnaire

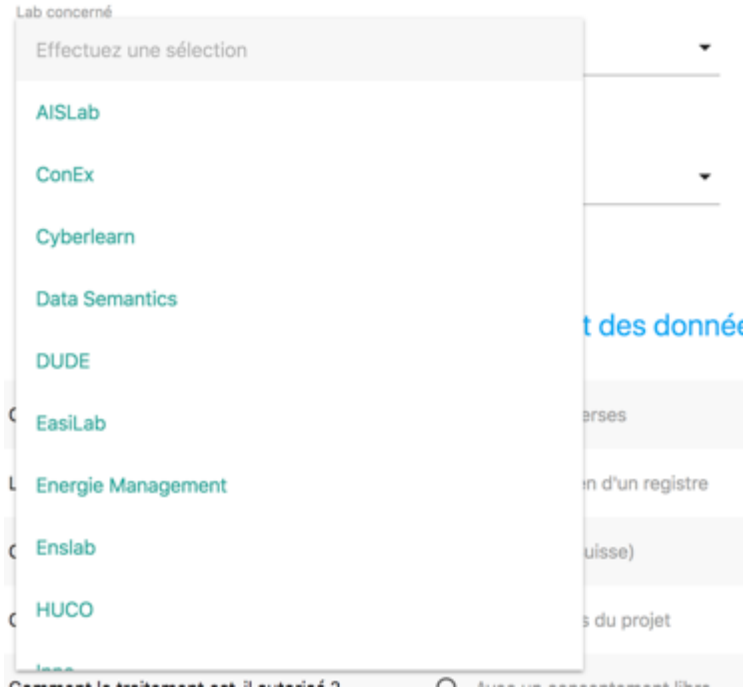


Source : (Données de l'auteur, 2018)

4.2.1. Lab concerné

Dans un premier temps, il peut sélectionner le lab de l'institut concerné par le traitement des données. En règle générale, les instituts sont structurés selon plusieurs labs qui opèrent de manière autonome selon leur activité. Cette sélection est donc propre au cas d'utilisation de notre outil au niveau des instituts.

Figure 26 : Sélection d'un lab



Source : (Données de l'auteur, 2018)

Les différents labs actuels des institut IIG et IEM ont été ajoutés dans ce prototype. Il n'est pas obligatoire de choisir un lab concerné par le traitement, car le résultat ne sera pas influencé par ce choix.

4.2.2. Type de données

Le type de données relatif au traitement peut influer sur divers aspects au regard des lois. De ce fait, l'utilisateur doit obligatoirement sélectionner un des trois types de données :

- Personnelles, correspondant aux données personnelles définies légalement
- Sensibles, correspondant aux données sensibles définies légalement
- Les deux, si le traitement regroupe des données personnelles et sensibles

Figure 27 : Sélection du type de données

Source : (Données de l'auteur, 2018)

4.2.3. Responsable de traitement

Indépendamment du type de données ou du lab, les données traitées peuvent être rattachées à une personne responsable de traitement. C'est la personne qui gère la façon dont les données sont traitées.

Pour ce prototype, deux responsables de traitement ont été désignés :

- Alexandre Cotting, pour l'institut IIG
- Francesco Cimmino, pour l'institut IEM

Figure 28 : Sélection du responsable de traitement

Source : (Données de l'auteur, 2018)

Ces responsables de traitement sont les personnes interviewées pour nos États de l'Art. Nous avons également pris en compte le fait qu'un responsable de traitement pourrait ne pas encore être défini dans la structure de l'institut, son choix est donc par défaut réglé à « Aucun » et facultatif.

4.2.4. Traitement des données défini légalement

Ce dernier *bloc* regroupe sous forme de tableau les différentes questions importantes au regard des textes légaux qui seront donc déterminants pour la vue des résultats. Il est important de prendre en compte le fait que ces questions ont été définies d'un point de vue purement légal et se rapportent uniquement aux articles de lois.

Six questions ont été considérées comme pertinentes et trois choix sont systématiquement proposés pour chacune d'entre elles :

1. **Quelles données sont traitées ?** Données diverses / Données anonymes / Seulement les données nécessaires
2. **Les données traitées sont-elles répertoriées ?** Oui, au moyen d'un registre / Vaguement / Non, pas du tout
3. **Où les données sont-elles stockées ?** À l'interne (Suisse) / À l'externe (sous-traitant) / À l'interne + une sauvegarde externe
4. **Qui a accès aux données stockées ?** Les membres du projet / Les collaborateurs du Lab / Accès libre (publique)
5. **Comment le traitement est-il autorisé ?** Avec un consentement libre / Avec un consentement présumé / Sans consentement requis
6. **Pourquoi est fait le traitement ?** Dans un but précis fixe / Dans un but qui pourrait évoluer / Sans but précis et mentionné

Figure 29 : Questions et choix

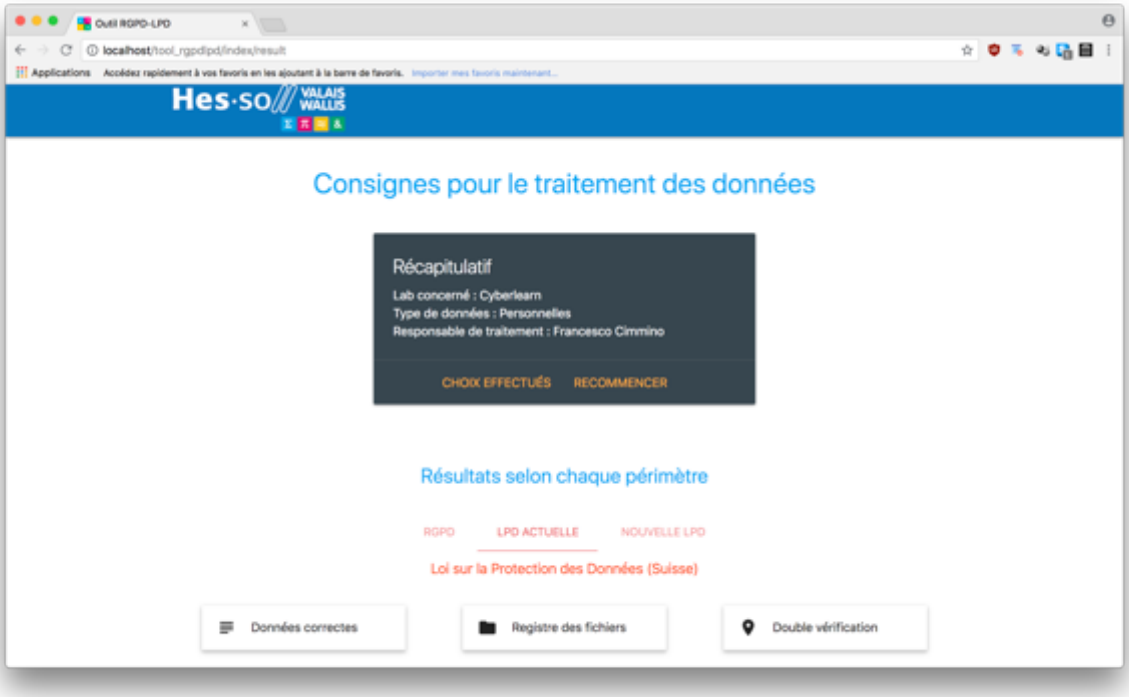
Source : (Données de l'auteur, 2018)

Pour valider le formulaire, il est obligatoire de répondre à toutes les questions et une unique réponse peut être cochée pour chaque question.

4.3. Vue du Résultat (Outputs)

Après avoir renseigné tous les champs dans la vue précédente, l'utilisateur est redirigé vers cette vue, séparée aussi en deux *blocs* distincts, qui lui affiche un résumé des informations entrées précédemment ainsi qu'un résultat, pour chaque réponse donnée aux six questions, selon les trois périmètres légaux, soit le RGPD, la LPD actuelle et le projet de révision de la LPD. De ce fait, l'utilisateur pourra sans problème retrouver les informations et choix qu'il a adoptés et les comparer avec les résultats.

Figure 30 : Vue des résultats

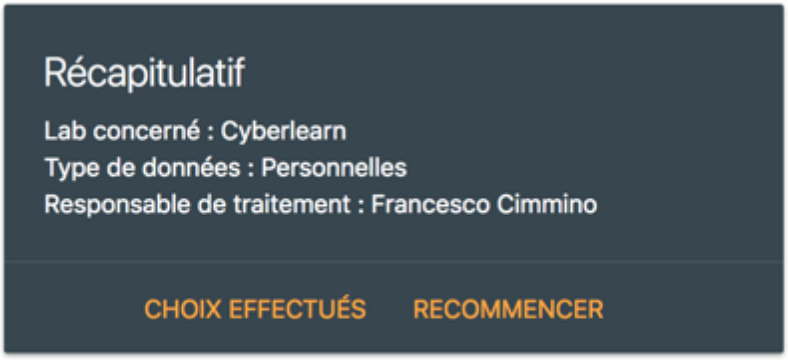


Source : (Données de l'auteur, 2018)

4.3.1. Récapitulatif

Un récapitulatif des informations insérées, présenté sous forme de « carte », est tout d'abord proposé. Il renseigne les sélections pour le lab concerné, le type de données ainsi que l'éventuel responsable de traitement.

Figure 31 : Récapitulatif des sélections

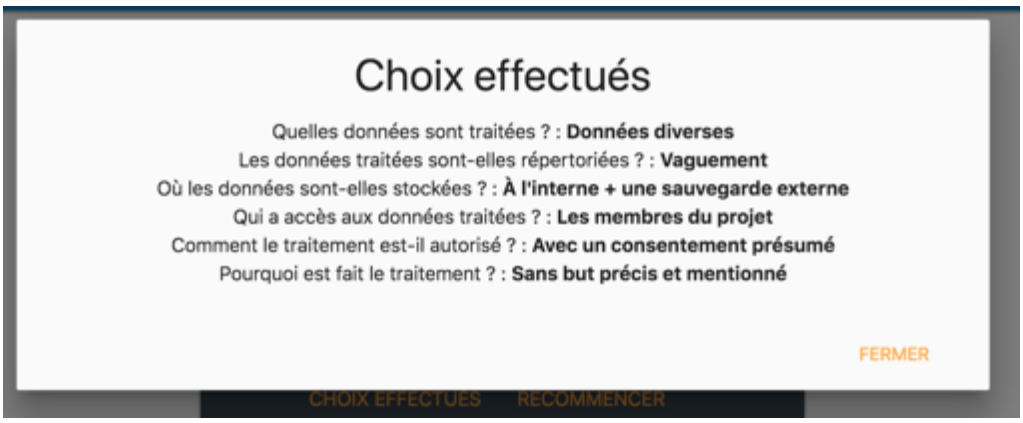


Source : (Données de l'auteur, 2018)

4.3.2. Bouton Choix effectués

Un premier bouton « Choix effectués » est situé en bas de la « carte », à gauche. Il affiche une fenêtre intégrée à la page web. Les questions posées et les réponses cochées précédemment sont sauvegardées par le site web et affichées à l'utilisateur. Le bouton « Fermer » permet de quitter la fenêtre afin de visualiser à nouveau la vue complète.

Figure 32 : Fenêtre des choix effectués



Source : (Données de l'auteur, 2018)

4.3.3. Bouton Recommencer

Également situé en bas de la « carte », mais à droite, un deuxième bouton « Recommencer » offre la possibilité à l'utilisateur de recommencer complètement le processus avec des informations différentes, relatives à un autre traitement, par exemple. Une fenêtre intégrée à la page web va s'afficher afin de pouvoir confirmer l'opération ou l'annuler. Cette mesure a été mise en place afin d'éviter que l'utilisateur « perde » tous les résultats en cliquant par erreur sur ce bouton.

Figure 33 : Fenêtre pour recommencer

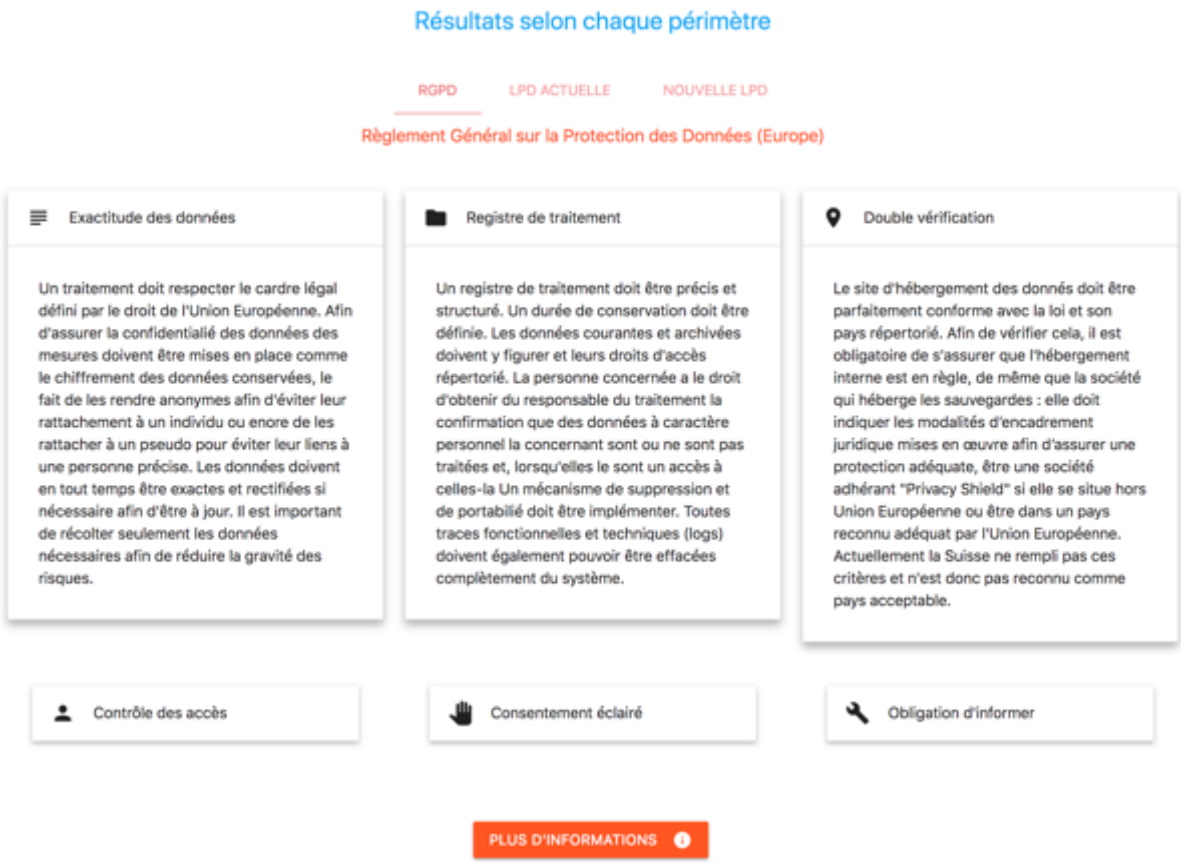
Source : (Données de l'auteur, 2018)

4.3.4. Résultats selon chaque périmètre

Les résultats sont finalement proposés et séparés selon les trois périmètres légaux (RGPD, LPD et « nouvelle » LPD). Pour rendre cela possible, trois *tabs* ont été implémentées. Elles sont dynamiques et leur contenu change automatiquement, sans qu'il soit nécessaire de recharger la page web.

Chaque résultat possède une icône, une catégorie et un texte de recommandation. Il correspond à une réponse donnée, à une question. Une icône et une catégorie ont été plébiscitées afin d'éviter que l'utilisateur s'égare si un résultat peut être scindé en plusieurs points. Ainsi, si un résultat comporte plusieurs recommandations, les cases correspondantes possèdent la même icône pour notifier que cela est relatif à la même question ; toutefois ils ont un libellé de catégorie et un texte différents. Dans l'implémentation de notre outil, seulement un résultat a été retenu pour chaque question.

Figure 34 : Affichage des résultats selon chaque périmètre



Source : (Données de l'auteur, 2018)

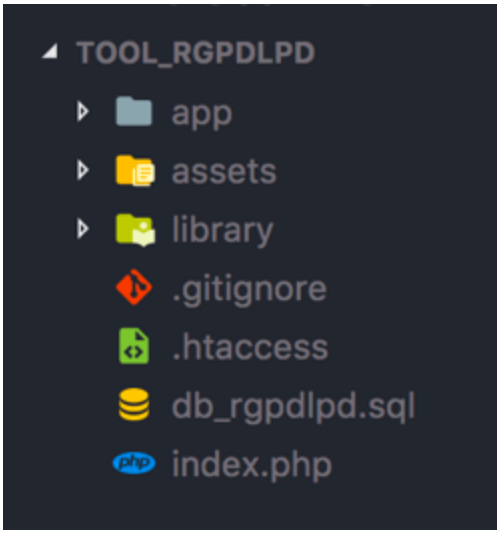
Un bouton « Plus d'informations » est disponible au fond de chaque résultat selon le périmètre. Il peut rediriger l'utilisateur vers le site de la confédération suisse ainsi que sur *GDPR made searchable by Algolia*[3], une plateforme qui regroupe les articles légaux de la RGPD et permet une recherche par mots clés dans ceux-ci.

4.4. Structure de l'outil

Comme déjà évoquée dans ce rapport, une structure *MVC* a été définie pour le développement de l'outil.

[3] GDPR made searchable by Algolia. Chapters, articles and recitals easily readable, https://gdpr.algolia.com/fr/

Figure 35 : Structure des répertoires et fichiers de l'outil

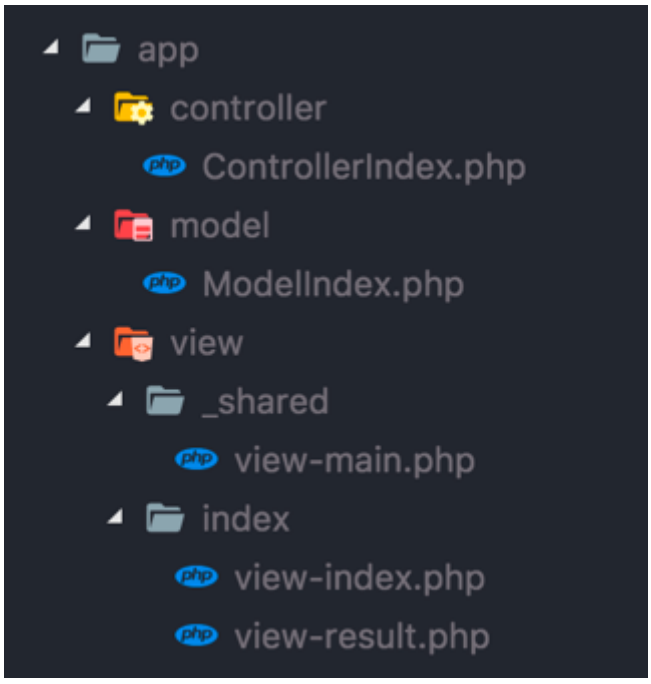


Source : (Données de l'auteur, 2018)

Afin de respecter cette manière de conception, trois répertoires sont structurés :

- « app » regroupe des classes PHP relatives au *MVC* soit le modèle, le contrôleur et les vues (avec le code HTML)

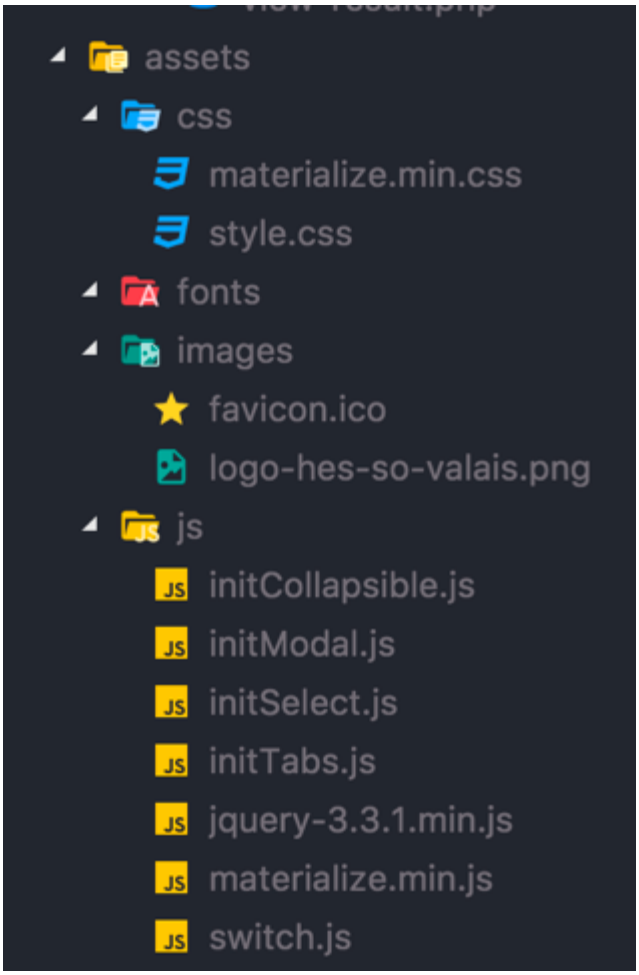
Figure 36 : Dossier "app" de la structure de l'outil



Source : (Données de l'auteur, 2018)

- « assets » englobe les fichiers de style CSS (dont le *Framework* « Materialize »), les images ainsi que les différents scripts (JavaScript pour initialiser les éléments graphiques et la bibliothèque JQuery)

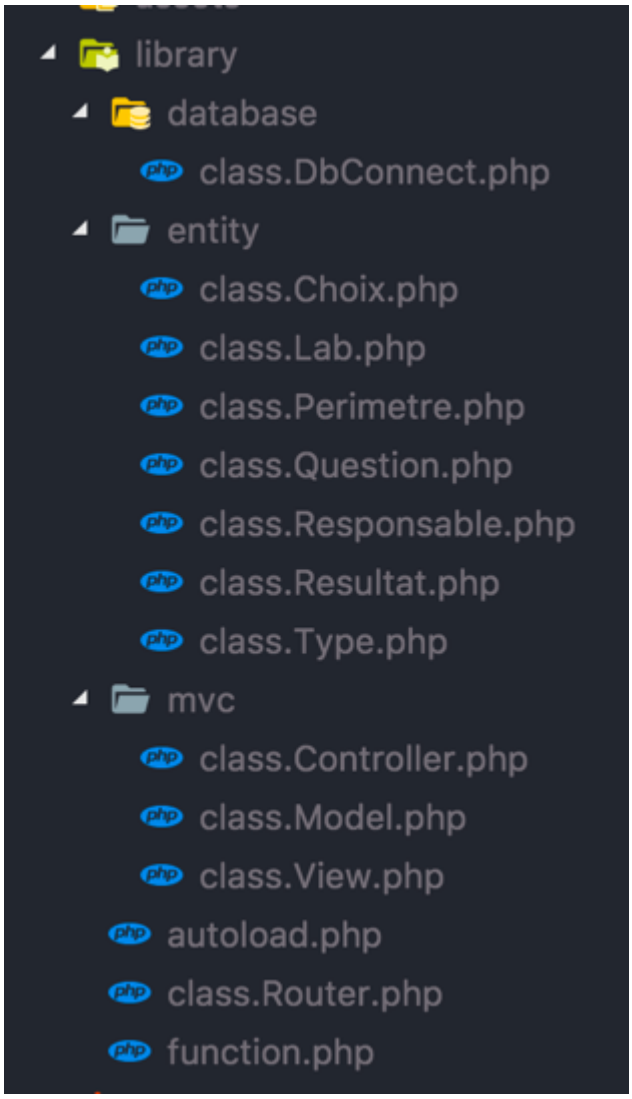
Figure 37 : Dossier "assets" de la structure de l'outil



Source : (Données de l'auteur, 2018)

- « library » contient toutes les classes qui permettent le fonctionnement du site web, soit les entités relatives aux tables de la base de données, les classes parentes de la structure *MVC* ainsi que le routeur qui va s'occuper de charger la page demandée

Figure 38 : Dossier "library" de la structure de l'outil

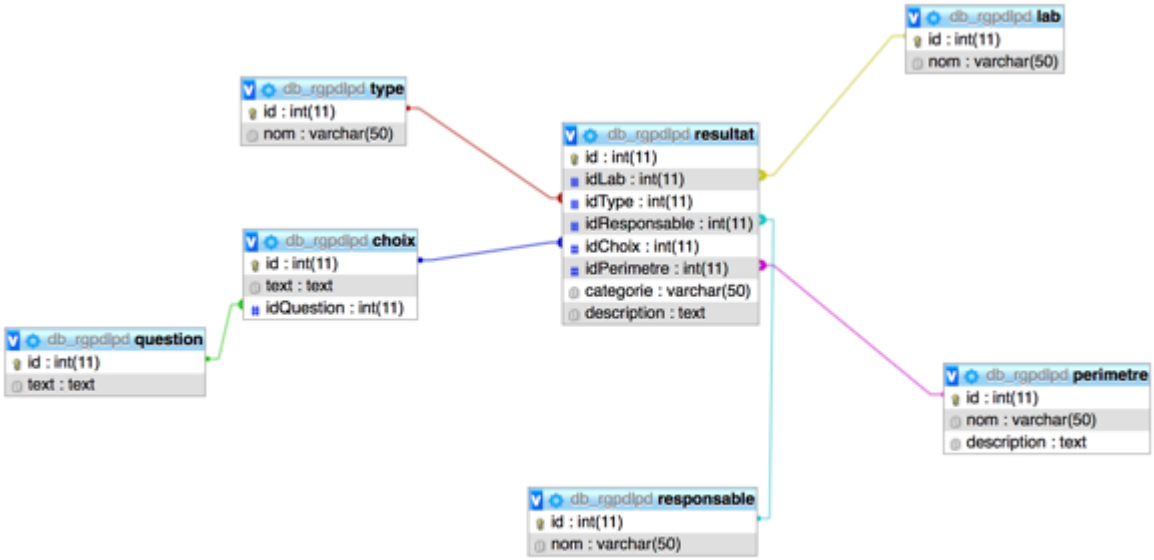


Source : (Données de l'auteur, 2018)

4.5. Base de données

La base de données de l'outil comprend sept tables.

Figure 39 : Schéma de la base de données



Source : (Données de l'auteur, 2018)

4.5.1. Table Lab

La table « lab » contient les noms des labs des instituts.

Figure 40 : Structure de la table "lab" dans la base de données

#	Nom	Type	Interclassement	Attributs	Null	Valeur par défaut	Commentaires	Extra
1	id	int(11)			Non	*Aucun(e)*		AUTO_INCREMENT
2	nom	varchar(50)	latin1_swedish_ci		Non	*Aucun(e)*		

Source : (Données de l'auteur, 2018)

4.5.2. Table Type

La table « type » contient les noms des différents types de données.

Figure 41 : Structure de la table "type" dans la base de données

#	Nom	Type	Interclassement	Attributs	Null	Valeur par défaut	Commentaires	Extra
1	id	int(11)			Non	*Aucun(e)*		AUTO_INCREMENT
2	nom	varchar(50)	latin1_swedish_ci		Non	*Aucun(e)*		

Source : (Données de l'auteur, 2018)

4.5.3. Table Responsable

La table « responsable » contient les noms des responsables de traitement.

Figure 42 : Structure de la table "responsable" dans la base de données

	#	Nom	Type	Interclassement	Attributs	Null	Valeur par défaut	Commentaires	Extra
☐	1	**id** 🔑	int(11)			Non	*Aucun(e)*		AUTO_INCREMENT
☐	2	**nom**	varchar(50)	latin1_swedish_ci		Non	*Aucun(e)*		

Source : (Données de l'auteur, 2018)

4.5.4. Tables Question et Choix

La table « question » répertorie tous les textes relatifs à chaque question. Elle est rattachée à la table « choix » qui contient les textes des différents choix. Afin de définir dans la base de données quels choix se rapportent à chaque question, un lien entre ces deux tables est nécessaire.

Figure 43 : Structure de la table "question" dans la base de données

	#	Nom	Type	Interclassement	Attributs	Null	Valeur par défaut	Commentaires	Extra
☐	1	**id** 🔑	int(11)			Non	*Aucun(e)*		AUTO_INCREMENT
☐	2	**text**	text	latin1_swedish_ci		Non	*Aucun(e)*		

Source : (Données de l'auteur, 2018)

Figure 44 : Structure de la table "choix" dans la base de données

	#	Nom	Type	Interclassement	Attributs	Null	Valeur par défaut	Commentaires	Extra
☐	1	**id** 🔑	int(11)			Non	*Aucun(e)*		AUTO_INCREMENT
☐	2	**text**	text	latin1_swedish_ci		Non	*Aucun(e)*		
☐	3	**idQuestion** 🔗	int(11)			Non	*Aucun(e)*		

Source : (Données de l'auteur, 2018)

4.5.5. Table Périmètre

La table « perimetre » contient les noms (abréviations) des différents périmètres légaux et leurs descriptions (noms complets).

Figure 45 : Structure de la table "perimetre" dans la base de données

#	Nom	Type	Interclassement	Attributs	Null	Valeur par défaut	Commentaires	Extra
1	id	int(11)			Non	*Aucun(e)*		AUTO_INCREMENT
2	nom	varchar(50)	latin1_swedish_ci		Non	*Aucun(e)*		
3	description	text	latin1_swedish_ci		Non	*Aucun(e)*		

Source : (Données de l'auteur, 2018)

4.5.6. Table Résultat

Enfin, la table « resultat » comporte toutes les catégories et descriptions des résultats. Cette table est liée aux tables « lab », « type », « responsable » et « choix ». Un résultat avec sa catégorie et sa description peut donc être ressorti selon un lab concerné, un type des données, un responsable de traitements et une réponse cochée.

Figure 46 : Structure de la table "resultat" dans la base de données

#	Nom	Type	Interclassement	Attributs	Null	Valeur par défaut	Commentaires	Extra
1	id	int(11)			Non	*Aucun(e)*		AUTO_INCREMENT
2	idLab	int(11)			Oui	*Aucun(e)*		
3	idType	int(11)			Non	*Aucun(e)*		
4	idResponsable	int(11)			Oui	*Aucun(e)*		
5	idChoix	int(11)			Non	*Aucun(e)*		
6	idPerimetre	int(11)			Non	*Aucun(e)*		
7	categorie	varchar(50)	latin1_swedish_ci		Non	*Aucun(e)*		
8	description	text	latin1_swedish_ci		Non	*Aucun(e)*		

Source : (Données de l'auteur, 2018)

Pour l'utilisation de notre prototype, le lab concerné et le responsable de traitements ne sont jamais sollicités, c'est pour cette raison que leur valeur peut être vide (colonne « Null »).

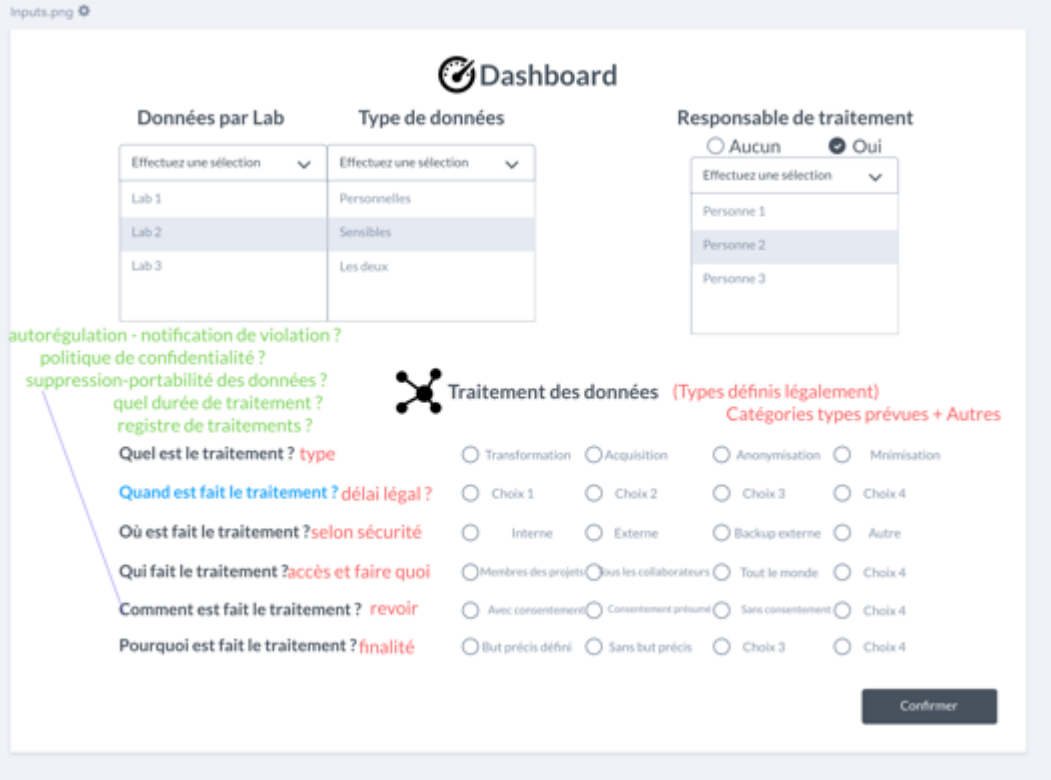
5. Use cases réalisés

Une fois le développement de l'outil finalisé, il a fallu insérer différents cas d'utilisation qui définissent les données d'insertion (inputs) de l'utilisateur et les résultats qui lui seront proposés (*outputs*). Une phase conséquente d'analyse de ces données a démarré dès le début de la conception de l'outil, lors de la réalisation évoquée précédemment des *mock-up*.

5.1. Inputs

Étant donné les subtilités légales, les différentes questions ont été amenées à évoluer durant tout ce processus. En effet, ces questions constituent la base pour les résultats qui seront proposés. Il est donc primordial qu'elles soient pertinentes, claires et précises. Aussi, dès qu'elles sont validées, l'analyse pour leur choix de réponses peut débuter.

Figure 47 : Mock-up évolué de la vue "inputs"



Source : (Données de l'auteur, 2018)

Les six principales questions, imagées dans le *mock-up* ci-dessus, ont servi de base durant toute la phase d'analyse des textes légaux et ont été amenées à évoluer pour la solution finale, présentée au point 4.2 de notre rapport. Leurs logiques sont décrites ci-dessous avec une description de leurs choix.

Tableau 3 : Précisions aux choix des questions (inputs)

Questions	Choix 1	Choix 2	Choix 3
Quelles données sont traitées ?	Données diverses : Toutes les données sont stockées sans faire aucune différentiation de leur type ou caractéristique	Données anonymes : Les données sont anonymes, la personne concernée ne peut être facilement reconnaissable et ses données rattachées à elle-même	Données nécessaires uniquement : Un effort est fait en ne récoltant que les données purement nécessaires au fonctionnement du projet (minimum)
Les données traitées sont-elles répertoriées ?	Oui, au moyen d'un registre : Un registre de traitement est maintenu afin de référencer toutes les données, de leur provenance à leur durée de conservation	Vaguement : Les données sont répertoriées de façon non structurée, propre à chaque projet ou chercheur	Non, pas du tout : Aucune mesure n'a été prise afin de répertorier les données
Où les données sont-elles stockées ?	À l'interne (Suisse) : Les données sont stockées dans les systèmes d'information du lab ou de l'institut	À l'externe (sous-traitant) : Un sous-traitant héberge les données	À l'interne + une sauvegarde externe : En plus de stocker les données à l'interne, une copie est hébergée chez un sous-traitant
Qui a accès aux données traitées ?	Les membres du projet : Seulement les membres relatifs au projet ont accès aux données, leur nombre est donc réduit	Les collaborateurs du lab : Tous les collaborateurs du lab peuvent accéder aux données, le nombre d'accès est donc augmenté	Accès libre (publique) : Les données sont accessibles publiquement

Comment le traitement est-il autorisé ?	Avec un consentement libre : La personne concernée a un choix total de refuser ou d'accepter la collecte de ses données qui lui est proposée explicitement	Avec un consentement présumé : Le consentement de la personne concernée et implicite, on présume qu'il accepte en pré cochant une case par exemple	Sans consentement requis : Aucun consentement n'est demandé à la personne concernée, ses données sont tout de même collectées
Pourquoi est fait le traitement ?	Dans un but précis et fixe : La finalité du traitement est clairement exprimée et elle n'ira pas au-delà	Dans un but qui pourrait évoluer : La finalité du traitement est présentée, mais elle pourrait évoluer après que la personne concernée l'ait acceptée	Sans but précis et mentionné : Aucune finalité de traitement n'est évoquée, les données sont tout de même collectées

5.2. Outputs

Après avoir terminé l'étape d'analyse des *inputs*, nous avons évalué les différents résultats qui pourraient être disponibles à l'utilisateur. Pour cela, nous avons décidé qu'ils seraient, dans un premier temps, influencés par les choix. En prenant compte qu'un choix donnera une réponse, le nombre de réponses s'élève donc à 18 cas. Il faut ensuite ajouter à ce total le fait que les réponses doivent correspondre à trois périmètres distincts (RGPD, LPD, projet de révision LPD). Le nombre de réponses est ainsi multiplié par 3, ce qui résulte de 54 cas possibles. Enfin, nous avons pris en compte le type de données traitées (sensibles, personnelles ou les 2) car il est souvent abordé dans les lois. Une multiplication supplémentaire retourne donc une possibilité finale de 162 résultats.

Figure 48 : Possibilités de résultats pour les données personnelles

Source : (Données de l'auteur, 2018)

Tous les résultats que nous avons retenus et insérés dans la base de données sont disponibles sur le CD-ROM joint à ce rapport, sous forme de tableau dans le fichier Excel « 01_Uses_Cases.xlsx ».

6. Conclusion

6.1. Synthèse générale

L'idée principale de ce travail était de démontrer, après avoir analysé les différents textes légaux et les outils d'accompagnement disponibles sur le marché, où se situait la HES-SO Valais, et plus précisément ses instituts de « Recherche et Développement », et de lui proposer un prototype d'outil présentant une approche choisie qui pourrait permettre d'accompagner son futur DPO dans ses tâches.

Après avoir, dans un premier temps, démontré l'état purement juridique de ses textes légaux, nous avons pu observer que les devoirs d'une institution comme la HES-SO Valais sont conséquents afin d'assurer une conformité totale. Ces textes sont relativement récents ou encore en cours d'élaboration et leurs principes de protections des données, champs d'application et sanctions sont relativement pointus et nouveaux, même à une ère comme la nôtre, où internet et le traitement des données ont pris une place prépondérante dans notre quotidien.

Nous constatons clairement, que les mesures n'ont pas été légiféré graduellement et cette situation amène donc à une certaine prise de conscience soudaine des entreprises, imposée par les diverses institutions, qui se résulte d'une certaine « panique » dans tous les secteurs. Il a aussi été intéressant de remarquer l'écart entre la LPD suisse, qui date principalement de 1992, et son projet de révision toujours en cours d'élaboration.

Dans un second temps, nous avons observé les outils d'accompagnement aux entreprises et constaté qu'une multitude d'approches étaient possibles afin d'aider aux mieux tout type d'entreprises. Le fait que ces outils étaient principalement axés sur la RGPD européenne nous a, encore une fois, permis de noter que la Suisse avait un énorme retard en matière de protection des données. Il a été, enfin, intéressant de s'apercevoir qu'un poste complètement nouveau de DPO a été mis en place pour une structure d'entreprise actuelle. Cela nous a prouvé que les enjeux étaient conséquents et que toutes ces questions de traitements des données étaient prises au sérieux par les différents acteurs. Si, actuellement, ces changements sont difficiles à entreprendre, il ne fait aucun doute qu'ils seront fondamentaux dans un avenir proche.

Après avoir consulté des collaborateurs d'instituts, nous avons pu observer que la conformité de ces instituts n'est, à leur connaissance, pas assurée. Nous constatons qu'aucune ligne directrice claire ne leur a été donnée et que, de ce fait, aucune réelle démarche n'est en cours, malgré le fait qu'ils collaborent fréquemment avec des établissements basés en Union Européenne dans leurs projets.

En conclusion, l'outil réalisé nous a permis de démontrer un type de fonctionnement possible à l'interne et l'utilité qu'il pourrait apporter au futur DPO de la HES-SO Valais.

6.2. Avis personnel

J'ai, personnellement, beaucoup apprécié réaliser ce travail. En effet, j'ai toujours été intéressé par la manière dont les entreprises et institutions géraient nos données collectées sur internet. Mon impression a globalement toujours été que celles-ci ne portaient aucune attention particulière au traitement de ces données et que, finalement, le seul moyen pour l'utilisateur qui s'en souciait était de purement arrêter d'utiliser ces services en ligne.

Ce travail m'a permis de prendre connaissance concrètement des textes légaux et de mieux me positionner sur les traitements quotidiens qui me concernent avec les applications, téléphones portables et systèmes d'exploitation. Je suis ravi que nos institutions se penchent enfin sur ces questions très sérieuses qui résultent de l'explosion de l'utilisation d'internet dans notre quotidien. L'aboutissement de ces règlementations prouve malheureusement qu'il faut forcer la main aux grandes compagnies *high-tech* pour qu'elles prennent enfin des mesures nécessaires afin de protéger au mieux les personnes concernées.

La réalisation de l'outil *Proof of Concept* s'est dans l'ensemble déroulée sans embûches. La partie qui m'a demandé le plus de réflexions et de temps est, sans aucun doute, celle des résultats à introduire dans l'outil (*outputs*). Cela prouve que la réalisation dans les démarches à la mise en conformité doit impérativement se faire de manière transversale entre la technique, qui était mon domaine, le juridique et l'organisationnel.

6.3. Cahier des Charges

Tous les principaux objectifs mentionnés dans le cahier des charges ont été atteints.

Il a été très complexe de rédiger un cahier des charges clair et précis dès le début de la réalisation de ce travail. En effet, la situation de la HES-SO a beaucoup évolué tout au long de ce travail étant donnée la situation relativement récente des textes légaux. À ses débuts, ce travail était censé concerner plus généralement la HES-SO. La décision de celle-ci de mandater une entreprise externe nous a ainsi obligés à nous concentrer sur la HES-SO Valais et, respectivement, les instituts « Recherche et Développement ».

Les rapports visant à indiquer les écarts et solutions ainsi que le fait de démontrer l'utilisation de l'outil n'ont, par conséquent, pas été complètement abordés. Cela résulte de la complexité réelle de ces analyses avec des démarches qui doivent être entreprises à l'interne et dans tous les secteurs qui n'auraient pas pu être réalisables dans le temps imparti de ce travail. Celles-ci vont être réalisées dans les mois à venir par la HES-SO Valais avec la mise en place d'un DPO, la nomination d'un nouveau responsable du service informatique et l'appui juridique de Mme Natacha Albrecht.

6.4. Améliorations possibles

Comme il a été explicitement défini dès le début de ce travail, l'outil réalisé est uniquement un prototype qui vise à démontrer une approche réalisable, afin de vérifier la conformité légale des instituts. Ses possibilités d'améliorations sont donc multiples.

En partant du principe que la base de cet outil sera conservée, une amélioration technique devrait être faite sur la partie qui concerne son administration. En effet, dans l'état, il est uniquement possible de modifier des questions, choix et résultats depuis la base de données, au moyen de requêtes SQL. Une interface utilisateur (vue) « Administration » offrirait donc le moyen au DPO d'ajuster simplement ces données selon les cas de figure qui se présentent. Une fonctionnalité intéressante serait aussi d'offrir la possibilité d'exporter directement les résultats en format informatique (Excel ou csv par exemple) afin qu'ils soient archivés ou réutilisés en cas de besoins.

Au niveau de la conception, il serait également plus approprié de sélectionner le périmètre légal concerné avant même de répondre aux questions et de sélectionner des choix. Les réponses aux questions à cocher pourraient être beaucoup plus pertinentes selon les articles de loi du périmètre et le résultat, donné à l'utilisateur, plus clairvoyant.

Pour une utilité destinée aux instituts, j'ai aussi trouvé intéressant certaines remarques reçues en retour comme le fait de préciser les caractéristiques des données, le nombre de personnes concernées qui donnerait une idée de la taille du *DataSet* ainsi que la source de ces données.

Enfin, les résultats proposés par l'outil pourraient être donnés de manière plus automatisée, au moyen d'algorithmes ou de technologies plus récentes comme l'intelligence artificielle que nous avons évoquée dans notre État de l'Art technique. Ainsi, l'outil adapterait ses réponses en considérant réellement tous les choix sélectionnés et non plus en faisant correspondre par défaut un résultat à un choix. La réponse donnée à la première question influerait donc sur la deuxième, par exemple.

RÉFÉRENCES

Albrecht, N. (2018). *Analyse générale de l'applicabilité de la RGPD, de la LPD et/ou de la LIPDA au niveau de la direction de l'Etat major de la HES-SO Valais/Wallis.*

ALiveVam. (2018, Mai 22). *What is PHP?How to write a PHP program*. Récupéré sur NoobsPlanet: https://noobsplanet.com/index.php?threads/what-is-php-how-to-write-a-php-program.230/

alternativeTo. (2018). *Visual Studio Code*. Récupéré sur alternativeTo: https://alternativeto.net/software/visual-studio-code/

Apache Friends. (2018). *XAMPP Installers and Downloads for Apache Friends*. Récupéré sur Apache Friends: https://www.apachefriends.org/fr/index.html

Arya, A. (2017, Octobre 20). *What is the relationship between HTML, JavaScript and CSS?* Récupéré sur Quora: https://www.quora.com/What-is-the-relationship-between-HTML-JavaScript-and-CSS

Assemblée fédérale de la Confédération suisse. (1992, Juin 19). *Loi fédérale sur la protection des données (LPD)*. Récupéré sur admin.ch: https://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf

Biseul, X. (2018, Avril 24). *11 outils logiciels pour accélérer la mise en conformité au RGPD*. Récupéré sur ZDNet: https://www.zdnet.fr/actualites/11-outils-logiciels-pour-accelerer-la-mise-en-conformite-au-rgpd-39867444.htm

BookMyEssay. (2018). *Online MySQL Database Assignment Help*. Récupéré sur BookMyEssay: https://www.bookmyessay.com/mysql-database-assignment/

Canton du Valais. (s.d.). *LOI SUR L'INFORMATION, LA PROTECTION DES DONNÉES ET L'ARCHIVAGE*. Récupéré sur vs.ch: https://www.vs.ch/web/che/lipda

Cimmino, F. (2018, Juillet 9). Phd- Research Assistant Insitut IEM, HES-SO Valais-Wallis. (P. Clivaz, Intervieweur)

Cleveroad. (2018). *Get Ready for General Data Protection Regulation*. Récupéré sur GDPR Compliance Checklist: https://www.cleveroad.com/gdpr-compliance-checklist/

CNIL. (2017, Mars 2). *Organiser les processus internes*. Récupéré sur CNIL: https://www.cnil.fr/fr/organiser-les-processus-internes

CNIL. (2018). *La CNIL en France*. Récupéré sur CNIL: https://www.cnil.fr/fr/la-cnil-en-france

CNIL. (2018). *Le délégué à la protection des données (DPO)*. Récupéré sur CNIL: https://www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo

CNIL. (2018, Mai 31). *Outil PIA : téléchargez et installez le logiciel de la CNIL*. Récupéré sur CNIL: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

CNIL. (s.d.). *RGPD : se préparer en 6 étapes*. Récupéré sur CNIL: https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

Coheris. (2018). *A PROPOS*. Récupéré sur Données RGPD: https://donnees-rgpd.fr/a-propos/

Coheris. (2018). *RGPD TEXT-CONTROL*. Récupéré sur RGPD Text-Control - Identification automatique des données sensibles: https://donnees-rgpd.fr/rgpd-text-control/

Confédération Suisse. (2017, Août 10). *Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales*. Récupéré sur admin.ch: https://www.admin.ch/ch/f/gg/pc/documents/2826/Revision-totale-de-la-loi-sur-la-protection-des-donnees_Rapport-resultats_fr.pdf

Confédération suisse. (2017, Septembre 15). *Une meilleure protection des données et un renforcement de l'économie suisse*. Récupéré sur admin.ch: https://www.ejpd.admin.ch/ejpd/fr/home/aktuell/news/2017/2017-09-150.html

Cotting, A. (2018, Juin 25). Professeur et Collaborateur Institut Informatique de Gestion, HES-SO Valais-Wallis. (P. Clivaz, Intervieweur)

CUI Unige. (2018). *Responsable de la protection des données en entreprise / DPO*. Récupéré sur Séminaires CUI Unige: http://seminaires-cui.unige.ch/dpo

Data Protection Company. (2018). *DATA PROTECTION OFFICER*. Récupéré sur Data Protection Company: https://data-protection-agency.ch/dpo-externe/

(2018). *Données de l'auteur*.

econocom. (2018, Janvier 22). *DATA PROTECTION OFFICER (DPO) : LA FONCTION TRÈS RECHERCHÉE POUR LE RGPD*. Récupéré sur E-media.

Feed-backs de divers utilisateurs. (s.d.). *What are the best IDEs or editors for PHP?* Récupéré sur Slant: https://www.slant.co/topics/253/~best-ides-or-editors-for-php

Fockens, L. (2018, Avril 10). *8 Best Practices to Become an Effective Data Protection Officer (DPO)*. Récupéré sur everteam: https://www.everteam.com/en/8-best-practices-become-effective-data-protection-officer-dpo/

Frammery, C. (2018, Février 27). *Données personnelles: le sprint des entreprises suisses pour intégrer la loi européenne*. Récupéré sur Le Temps: https://www.letemps.ch/economie/donnees-personnelles-sprint-entreprises-suisses-integrer-loi-europeenne?utm_source=amp

Futura-Sciences. (2018). *MySQL*. Récupéré sur Futura Tech: https://www.futura-sciences.com/tech/definitions/internet-mysql-4640/

Garessus, E. (2017, Novembre 13). *La directive sur la protection des données sera le cauchemar de 2018*. Récupéré sur Le Temps: https://www.letemps.ch/economie/directive-protection-donnees-sera-cauchemar-2018

HES-SO. (2018). Conseil de domaine Economie et services. *Réglement RGPD*. Catherine Ingold Schuler.

HES-SO Valais-Wallis. (2017). *REMISE DE DIPLÔMES DE LA FILIÈRE TOURISME*. Récupéré sur HES-SO Valais-Wallis: https://www.hevs.ch/fr/hautes-ecoles/haute-ecole-de-gestion-et-tourisme/tourisme/events/remise-de-diplomes-de-la-filiere-tourisme-14465

HES-SO Valais-Wallis. (2018). *ADAPTER SON ENTREPRISE AU RGPD*. Récupéré sur HES-SO Valais-Wallis: https://www.hevs.ch/fr/hautes-ecoles/haute-ecole-de-gestion-et-tourisme/informatique-de-gestion/autres-formations/formation-continue/cours-entreprise-institution/formations-specifiques/adapter-son-entreprise-au-rgpd-18603

HES-SO, R. (2017). *Protection des données : Options d'organisation et de financement*.

IAPP. (2018). *Votre communauté mondiale et vos ressources les plus complètes en matière de confidentialité des informations*. Récupéré sur International Association of Privacy Professionals: https://iapp.org/lang/fr/

InfoWebMaster. (2018). *Javascript*. Récupéré sur Informations et ressources pour webmasters: http://glossaire.infowebmaster.fr/javascript/

Kellerhals Carrard. (2017, Février). *Règlement européen sur la protection des données - Ce que les entreprises suisses doivent savoir*. Récupéré sur Kellerhals Carrard: https://www.kellerhals-carrard.ch/upload/cms/user/KuB_2.2017fr.pdf

Kynapse. (2018, Avril 17). *L'Intelligence artificielle au service du RGPD : Kynapse lance son chatbot GDPRAdvisor*. Récupéré sur Medium: https://blog.kynapse.fr/lintelligence-artificielle-au-service-du-rgpd-kynapse-lance-gdpradvisor-d2cfb96fd1ae

Labate, A. (2018, Mai 25). Responsable de la Sécurité des Systèmes d'Information (RSSI), Groupe T2i. (P. Clivaz, Intervieweur)

Mailjet. (2018). *The Ultimate GDPR Quiz*. Récupéré sur The Ultimate GDPR Quiz: https://ultimategdprquiz.com

Materialize. (2018). *About*. Récupéré sur Materialize: https://materializecss.com/about.html

Materialize. (2018). *Getting Started*. Récupéré sur Materialize: https://materializecss.com/getting-started.html

Microsoft. (2018). *PHP programming in VS Code*. Récupéré sur Visual Studio Code: https://code.visualstudio.com/docs/languages/php

Mozilla. (2018). *CSS : Feuilles de style en cascade*. Récupéré sur MDN web docs: https://developer.mozilla.org/fr/docs/Web/CSS

Mozilla. (2018). *HTML (HyperText Markup Language)*. Récupéré sur MDN web docs: https://developer.mozilla.org/fr/docs/Web/HTML

Mozilla. (2018). *jQuery*. Récupéré sur MDN web docs: https://developer.mozilla.org/fr/docs/Glossaire/jQuery

Mozilla. (2018). *La théorie Modèle Vue Contrôleur*. Récupéré sur MDN web docs: https://developer.mozilla.org/fr/Apps/Build/Architecture_d_une_application_web_moderne/MVC_architecture

Mozilla. (2018). *Qu'est-ce que JavaScript ?* Récupéré sur À propos de JavaScript: https://developer.mozilla.org/fr/docs/Web/JavaScript/A_propos

ORYGA. (2018). *ORYGA mise en conformité au RGPD*. Récupéré sur ORYGA: https://www.oryga.com/logiciel-saas-rgpd/

Parlement européen et Conseil relatif à la protection des personnes physiques. (2018). *CHAPITRE I Dispositions générales Article 4. Définitions*. Récupéré sur GDPR Made searchable by Algolia: https://gdpr.algolia.com/fr/gdpr-article-4

Parlement européen et Conseil relatif à la protection des personnes physiques. (2018). *Table of content*. Récupéré sur GDPR Made searchable by Algolia: https://gdpr.algolia.com/fr/

Pintado, E. (2017, Décembre 18). *Intégrer les nouvelles règlementations relatives à la protection des données personnelles de manière pragmatique*. Récupéré sur navixia.

Product Hunt. (2018, Mai). *GDPR Resources*. Récupéré sur Product Hunt: https://www.producthunt.com/e/gdpr-resources

Slant. (2018). *What are the best IDEs or editors for PHP?* Récupéré sur Slant: https://www.slant.co/topics/253/~best-ides-or-editors-for-php

The PHP Group. (2018). *Qu'est ce que PHP?* Récupéré sur PHP: https://secure.php.net/manual/fr/intro-whatis.php

Varonis. (2018). *GDPR Data Security and Classification*. Récupéré sur GDPR PATTERNS: https://www.varonis.com/products/gdpr-software/

Varonis. (2018). *Logiciel de conformité au GDPR*. Récupéré sur Varonis: https://www.varonis.com/fr/produits/gdpr-software/

W3Schools. (s.d.). *HTML Editors*. Récupéré sur W3Schools: https://www.w3schools.com/Html/html_editors.asp

W3Techs. (2018, Juin). *Usage statistics and market share of PHP for websites*. Récupéré sur W3Techs: https://w3techs.com/technologies/details/pl-php/all/all

ybierling. (2016, Décembre 3). *XAMPP Apache cannot start Port 80 in use*. Récupéré sur ybierling: https://www.ybierling.com/v2/fr/2016/12/03/xampp-apache-cannot-start-port-80-in-use-2/

ANNEXES

ANNEXE 1 Cahier des Charges

Hes·so VALAIS WALLIS
Haute Ecole Spécialisée de Suisse occidentale
Fachhochschule Westschweiz
University of Applied Sciences Western Switzerland

FILIÈRE INFORMATIQUE DE GESTION

TRAVAIL DE BACHELOR
CAHIER DES CHARGES

Intégration de la RGPD et de la nouvelle LPD auprès des Instituts de « Recherche et Développement » de la HES-SO Valais

Mai 2018

Réalisé par Patrick Clivaz
Encadré par le professeur Bruno Montani

Hes·so

TABLE DES MATIÈRES

1. Contexte

Dans le cadre du travail de Bachelor, réalisé durant le 6e semestre de la filière Informatique de Gestion à la Haute École Spécialisée de Suisse occidentale (HES-SO) Valais-Wallis, le professeur Bruno Montani a proposé le sujet suivant : « Intégration de la RGPD et de la nouvelle LPD auprès des Instituts de « Recherche et Développement » de la HES-SO Valais ». L'étudiant a reçu la tâche d'effectuer un État de l'Art sur les lois « Règlement général sur la protection des données » (partie européenne) et « Loi sur la Protection des Données » (partie suisse) ainsi que de réaliser un outil qui facilitera la mise en conformité de ces lois dans le cadre de la HES-SO Valais, principalement dans le contexte des Instituts de Recherche et Développement.

Ce travail s'effectuera avec le soutien de Mme Natacha Albrecht, Avocate notaire et conseillère juridique auprès de la HES-SO Valais.

Le but de ce travail de Bachelor est, dans un premier temps, d'analyser les principaux articles de ces deux lois afin de cibler les ajustements essentiels que devra réaliser la HES-SO Valais pour assurer sa conformité dans les plus brefs délais. Puis dans un deuxième temps, un outil décisionnel sera réalisé afin de soutenir le DPO dans les mesures à mettre en place pour assurer une gestion des données adéquate selon leur utilisation et leur contexte au sein de la HES-SO Valais.

2. Description

Un cadre légal autour de la sécurité des systèmes d'information n'a jamais clairement été défini pour diverses raisons. Ce flou a longtemps permis aux différentes entreprises de gérer cette sécurité de manière aléatoire.

En 2016, la nouvelle Règlementation européenne pour la Protection des Données (RGPD) est entrée en vigueur et les entreprises concernées ont l'obligation de s'y mettre en conformité pour le 25 mai 2018. La Suisse a emboîté le pas de l'Union européenne en entamant une révision de la Loi sur la Protection des Données (LPD) en septembre 2017.

Le cadre règlementaire suisse actuel, basé sur la loi du 1er juin 1992, définit déjà un certain nombre de concepts et de règles qui servent aussi de base à la nouvelle règlementation européenne. Néanmoins, de nouvelles règles apparaissent et les nombreuses subtilités pourraient avoir des impacts importants sur les activités des entreprises.

2.1. Problématique concrète

Au vu de ces changements légaux en Europe et en Suisse, ce travail de Bachelor s'inscrit dans une analyse fine des adaptations auxquelles les entreprises vont devoir faire face ces prochains mois.

Hes·so

Quasiment toutes les entreprises suisses traitent, de manière informatisée ou non, des données qui tombent sous la loi européenne, respectivement suisse.

Malheureusement, la majorité des entreprises ne possèdent pas les moyens et/ou compétences pour se mettre en conformité avec ces lois, tant sous l'aspect technique que procédural.

La HES-SO Valais n'échappe pas à ces lois et ce travail de Bachelor vise à lui offrir un outil d'aide pour les différentes étapes à suivre, définies selon le contexte, le périmètre géographique (UE ou Suisse) ainsi que l'utilisation précise des données afin qu'elle puisse se mettre en conformité avec ces deux lois majeures.

3. Objectifs

Durant ce travail de Bachelor, l'étudiant sera amené à atteindre plusieurs objectifs :

- État de l'art des textes de loi de la RGPD et des lois LPD (texte actuel et projet de révision)
- État de l'art des outils d'analyse d'entreprise sous l'angle de la RGPD et LPD
- Identifier et classifier les données de la HES-SO Valais
- Créer un outil guidé et automatisé d'aide à la mise en conformité légale
- Illustrer par la mise en place de différents use cases au sein de la HES-SO Valais

4. Phases de Travail

La création de l'outil couvre les étapes suivantes.

Pour les États de l'Art, des informations pourront être échangées avec M. Lionel Engel, également étudiant à la HES-SO Valais, qui réalise un travail de Bachelor sur la même thématique.

4.1. État de l'art de la RGPD et de la LPD

Dans un premier temps, l'étudiant va faire une analyse des différentes lois sur la protection des données (européenne et suisse) afin de cibler plus précisément ses objectifs.

La loi suisse sur la Protection des Données (LPD) sera divisée en deux parties afin de distinguer la loi actuellement en vigueur et son projet de révision. Il sera ainsi intéressant d'observer le statut de cette future modification étant donné que son application n'est pas encore prévue à ce jour.

4.2. Similitudes et différences entre ces lois

L'étudiant va ensuite établir les différents points qui se coordonnent ou s'opposent dans ces textes de loi, tout en distinguant toujours l'actuelle loi suisse et son projet de révision.

Hes·so

À travers ce résultat, il comprendra mieux les enjeux qui vont principalement impacter les entreprises suisses.

4.3. État de l'art des outils d'accompagnement aux entreprises pour la mise en conformité

L'étudiant va lister les outils d'accompagnement aux entreprises qui permettent la mise en conformité à ces différentes lois. Le but de cette phase est d'observer les solutions et pratiques actuellement disponibles et utilisées par les entreprises pour respecter la mise en conformité à ces lois.

Un mémoire réalisé dans ce sens par Mme Natacha Albrecht, conseillère juridique auprès de la HES-SO Valais, pourra également servir de base d'analyse solide.

4.4. Construire un outil d'aide à la décision de traitement de données pour la HES-SO Valais

Après avoir défini le type d'outil souhaité, l'étudiant va effectuer des « mockups » de cet outil ainsi que la logique de navigation pour avoir une vision globale de l'outil. Il va également choisir l'infrastructure informatique pour la réalisation de cet outil.

Cette phase est très importante afin d'avoir une idée claire du résultat final.

Le développement de cet outil évolutif et automatisé va ensuite débuter selon les fonctionnalités et besoins nécessaires à la HES-SO Valais et de son DPO selon la définition fournie en annexe.

4.5. Créer les rapports visant à indiquer les écarts et les solutions

L'étudiant va dresser des rapports clairs et précis, basés sur l'analyse précédente, qui vont démontrer les différences et les solutions pour permettre l'application de ces lois dans le cadre de la HES-SO.

4.6. Démontrer l'utilisation et l'applicabilité de l'outil et des rapports

En lien avec différents uses case, l'étudiant va effectuer cette dernière phase qui devrait idéalement se réaliser tout au long du projet. Elle permettra d'établir une documentation du travail de Bachelor sous forme de rapport.

5. Informations complémentaires

5.1. Délais

Remise du rapport : **30 juillet 2018 à 12h00**

Défense : **6 septembre 2018 à 11h00**

Exposition publique : **20 septembre 2018, Silicon Valais**

5.2. Nom

Intégration de la RGPD et de la nouvelle LPD auprès des Instituts de « Recherche et Développement » de la HES-SO Valais

Sierre, le 8.06.2018

Bruno Montani
Professeur

Patrick Clivaz
Etudiant en Informatique de Gestion

Annexe – Cahier des Charges

Remarques
=========
- Sous l'angle de la loi c'est pas la données qui est importante, mais c'est le traitement qui est important.
    - Rôle: responsable de traitement

Fonctionnement de l'outil final (vision)
==
* Produit utile au DPO sous un format de dashboard *

* Le DPO fait de la saisie manuelle dans l'outil et en output on a des indicateurs de conformité pour chaque loi *

Input
- Identifier les services

- Identifier les données par service
    - public
    - confidentiel
    - top secret

- Identifier le responsable de traitement

- Identifier les traitements de ces données (QQOQCP)
    - quel est le traitement
    - quand est fait le traitement
    - ou est fait le traitement
    - qui fait le traitement
    - comment est fait le traitement
    - pourquoi est faite le traitement

Indicateur en output:
Connfronter cette données vis-à-vis de:
- LIPDA
- RGPD
- LPD
- nLPD

Identifier les écarts et les conformités

Evolutivité de l'outil en fonction de l'évolution

ANNEXE 2 Planning

DATES	DUREE	OBJECTIFS	DETAILS	RDV
26.04.18	**1 heure**	**Première rencontre**	**Explication plus détaillée sur le TB par le professeur**	**Bureau, Bellevue**
09.05.18	**1 heure**	**Organisation du Cahier des charges et agenda des séances**	**Discussion sur le périmètre et planification des séances**	**Bureau, Bellevue**
10.05.18 - 11.05.18	*2 jours*	*Ascension*	*Jours fériés*	*NO*
14.05.2018 - 17.05.18	4 jours	Ébauche du cahier des charges	Discussions, remarques, définition de l'outil	NO
17.05.18	**1 heure**	**Présentation du Cahier des Charges**	**Validation du cadre légal, le périmètre précis sera défini selon les décisions de la HES-SO**	**Bureau, Bellevue**
21.05.18 - 25.05.18	5 jours	Recherches et Analyses pour les États de l'Art	Lecture des textes de lois et actualités en relation	NO
25.05.18	**1 heure**	**Ajustement du cahier des charges, structure des États de l'Art**	**Le cahier des charges est relu et modifié**	**Mikado, Technopôle**
28.05.18	**1 heure**	**Interview**	**Interview avec un Responsable de la Sécurité des Systèmes d'Information (RSSI)**	**Groupe T2i, Technopôle**
29.05.18	1 jour	Début de la rédaction des États de l'Art relatifs aux lois	Le cadre légal à suivre est mis en place	NO
30.05.18	**1 heure**	**Définir le périmètre du travail correspondant à la HES-SO**	**Le périmètre du travail est défini selon les décisions internes de la HES-SO, les inputs et outputs de l'outil sont donnés**	**Bureau, Bellevue**
31.05.18	*2 jours*	*Fête Dieu*	*Jours fériés*	*NO*
04.06.18 – 07.06.18	4 jours	Ajustement des recherches selon le périmètre choisi, définition du concept relatif à l'outil	Ciblage des points clés à étudier légalement selon le périmètre défini	NO
07.06.18	**1 heure**	**Validation du cahier des charges**	**Le cahier des charges est validé et signé, le product owner est choisi, le périmètre est maintenant confirmé**	**Bureau, Bellevue**
11.06.18 - 14.06.18	4 jours	Mock-up de l'outil, définition de la structure de la base de données, rédaction	Le fonctionnement de l'outil et de ses données est défini (inputs et outputs), la rédaction des États de l'Art continue en parallèle	NO
14.06.18	**1 heure**	**Présentation du concept de l'outil et de l'organisation du travail**	**La méthode de travail est définie, le fonctionnement de l'outil (users stories) est validé**	**Bureau, Bellevue**
15.06.18 – 21.06.18	5 jours	Prendre connaissances des technologies à utiliser	État de l'Art technique : analyse des technologies disponibles et choix	NO
21.06.18	**1 heure**	**Discussion sur le langage et l'architecture : choix technique**	**Présentation des différentes possibilités disponibles, architecture à mettre en place pour l'outil et de ses données, justifications des choix**	**Bureau, Bellevue**
22.06.18	*1 jour*	*Examen semestriel*	*Examen semestriel final*	*NO*
25.06.18 - 04.07.18	9 jours	Installation de l'infrastructure et développement de la base de données	L'installation se fait en local et la base de données est implémentée	NO
28.06.18	**1 heure**	**Discussion sur les inputs et outputs de l'outil et du résultat fourni**	**Réflexion sur les modifications à entreprendre sur l'infrastructure pour que le résultat souhaité corresponde**	**Bureau, Bellevue**
04.07.18	**1 heure**	**Présentation de l'implémentation réalisée et discussion de modifications**	**L'outil est présenté dans l'état et les éventuels ajustements sont évoqués**	**Bureau, Bellevue**

05.07.18 – 13.07.18	7 jours	Ajustements du fonctionnement de l'outil, amélioration du design	Les ajustements définis sont réalisés, le design est finalisé	NO
12.07.18	**1 heure**	**Présentation de l'outil réalisé**	**L'outil est validé et des dernières modifications peuvent être demandées si nécessaire**	**Bureau, Bellevue**
16.07.18 – 20.07.18	5 jours	Tests de l'outil	Des tests sont réalisés sur l'outil et des dernières améliorations et corrections sont réalisées	NO
23.07.18 – 27.07.18	5 jours	Finalisation de la rédaction du rapport	Correction des textes, relecture, rapport adapté selon les résultats de l'outil	NO
27.07.18	**1 heure**	**Validation du travail réalisé**	**Discussion avec le professeur afin de valider le travail**	**Bureau, Bellevue**
30.07.18		Dépôt du travail	Le travail est rédigé, l'outil est fonctionnel : il est déposé avant 12h	Espace de rendu, Moodle
06.09.18	**1 heure**	**Défense orale**	**Défense orale du TB à 11h**	**A définir**

Remarque : tous les vendredis jusqu'au 8 juin, pas de travail car participation à l'option Business eXperience

ANNEXE 3 Interview T2i

Adriano Labate

Responsable de la Sécurité des Systèmes d'Information (RSSI)

adriano.labate@groupe-t2i.com

- Quels enjeux à T2i ? Quel impact sur les activités ?
  - 200 personnes qui travaillent à T2i, 100 à Sierre et Renens
  - Une filiale est en France et donc soumise au RGPD → Paris et Lyon
  - Très attentif au RGPD, un site se trouve dans l'UE et fournit des biens et services destinés aux citoyens européens
  - Des prestations de sous-traitant et d'hébergement sont proposées → risque de perte de marché énorme si non conforme
  - Un client européen doit être assuré que l'entreprise suisse est conforme au RGPD
  - Grand danger de réputation → s'il y a une mauvaise communication les clients sollicitent l'entreprise, si pas de réponse claire → contrat peut être cassé
  - Il faut communiquer, prendre les devants avant que le client le fasse !
  - Le délai de 2 ans défini par l'UE (2016 → 2018) est trop court et ridicule, pas mal de flous règnent encore, la loi est "jeune"
- Où trouver les "bonnes pratiques" à adopter ?

  3 aspects importants sont à prendre en compte :

  - Juridique : Suivre une formation → séminaire organisé par CUI Unige pour Responsable de la protection des données en entreprise / DPO, 7 jours de formation, bonnes bases LPD (actuelle / nouvelle) et RGPD
  - Technique : du développement et de la sécurité → compétence déjà présente dans l'entreprise
  - Organisationnel : il faut définir un rôle "officiel" dans l'entreprise, les clients se sentent ainsi rassurés, nécessité de retravailler tous les contrats, beaucoup de travail, ça coute très cher → avenant au contrat actuel pour informer cela (mesures de sécurité, les droits, politique de protection), les contrats ont été révisés en parallèle pour assurer la mise en conformité, le délai était très cours, un mandat a été donné à une société spécifique à cette mise en conformité
- Y'a-t-il des outils d'accompagnement pour entreprise ?
  - Des outils existent sur le marché, ces solutions n'ont pas été retenues, car c'est encore "jeune"
  - En général, ils ne sont pas encore très clairs
  - Outil PIA de la CNIL existe, il est trop détaillé et pas adapté selon l'entreprise
  - Une entreprise fournit un questionnaire en ligne et des juristes vont analyser les réponses pour proposer des solutions adéquates → peut-être une bonne solution
- Depuis quand le processus de mise en conformité a débuté ?
  - Février 2016, la direction a été alertée
  - Courant 2017, début concret du processus
  - Pas facile à mettre en place
  - Dans ce cas-là, j'étais seul, pas d'équipe → le responsable sécurité s'est formé en DPO
  - Il faut travailler avec tout le monde, vision transversale, sensibilisation à faire à l'interne
  - Les commerciaux, chefs de projets doivent "jouer le jeu" → transmettre au responsable les questions de clients
  - De grands investissements ont été réalisés
- Quelles solutions/mesures concrètes choisies ?

    - Très difficile avec les applications, certaines sont seulement maintenues
    - Très complexe selon les langages et conceptions différents, certains peuvent être obsolètes
    - L'objectif est de répondre au minimum dans ce cas, le droit d'accès et la suppression peuvent être réalisés manuellement, pas nécessairement dans l'application (du côté serveur par exemple) → cela répond au RGPD car la manière n'est pas précisée dans la loi
    - La plupart des applications le permettent
- Avez-vous un outil interne pour vérifier la mise en conformité GDPR ?
    - Au début, un rapport est créé avec des points prioritaires pour la démarche à réaliser → base de départ
    - Les démarches sont complexes généralement
- Appliquez-vous le principe du "Privacy by design" pour les projets actuels ?
    - C'est un aspect important
    - Cela peut être difficile dépend le langage/système
    - Encore une fois, des formation et sensibilisation doivent être réalisées
    - Ce principe va sans doute faire parti des futurs projets pour appliquer au mieux le RGPD
- Situation actuelle à T2i, y'a-t-il une distinction avec les projets en Suisse ou en UE ?
    - Les 2 sujets ont été adoptés
    - Naturellement, il y a différents contrats et avenants entre l'UE et la Suisse
    - Le but est de prendre les devants en Suisse → prévenir les clients
    - La RGPD et LPD actuelles ont de grandes différences → traiter au cas par cas
        - Le délai du devoir d'annonce est différent dans la loi
        - Limiter la collecte, le fait de s'opposer et la portabilité des données n'existent pas dans la loi suisse
- Quelle direction prendre en Suisse ?
    - L'aspect réputationnel est très important pour l'entreprise
    - Un client européen est mieux protégé qu'un client suisse → dommage
    - Une entreprise a meilleur temps de traiter tout le monde sur le même pied d'égalité → bonne pub
    - Autant "utiliser" ses obligations, car elles vont arriver → pour le marketing et l'image de l'entreprise (exemple récent de la Migros)
    - Les PME devraient s'y intéresser si les moyens le permettent
- Quels conseils pour, par exemple, la HES-SO ?
    - La même formation suivie que Mme Natacha Albrecht pour la HES-SO Valais
    - La GDPR doit être appliquée selon les statuts publique/privé en Suisse → les communes ne seraient pas soumises par exemple
        - Jurisprudence déjà à Neuchâtel et Jura
        - Les universités et HES sont soumises, car elles peuvent communiquer, attirer des étudiants/professeurs qui vivent au sein l'Union Européenne
        - Engager/former un DPO ?
            - Un DPO externe (mandat) peut très bien fonctionner si la charge n'est pas énorme
            - IAPP offre une certification pour DPO destiné à l'Europe

ANNEXE 4 Interview IIG

Alexandre Cotting

Professeur et Collaborateur à l'Institut Informatique de Gestion, HES-SO Valais-Wallis

alexandre.cotting@hevs.ch

- Quels enjeux pour l'institut IIG ? Quel impact sur les activités ?
  - Généralement → une incertitude et méconnaissance, beaucoup d'inconnus aujourd'hui
  - Enjeux au niveau de la recherche, surtout pour les projets européens : partenaires de recherches en Europe peuvent penser que la HES n'est pas compatible → perte de contact et de partenariat, les chances de financement sont réduites
  - Pas tous les chercheurs connaissent la loi, les projets existants ne sont pas vraiment compatibles, les bases de données ne sont pas adaptées, mais aucune analyse n'a été faite pour l'instant, les projets en cours ne doivent pas être arrêtés
  - Les chercheurs ne sont pas préparés actuellement, ça demande du temps pour assimiler les lois et répondre aux demandes
- Où trouver les "bonnes pratiques" à adopter ?
  - Attente sur la direction de l'école
  - Un petit speech a été fait à la séance d'institut récemment, un article sur la formation pour les développeurs et quelques cours en ligne pour se former ont été présentés, des indications sur les futurs rôles décisifs ont été précisées → Natacha Albrecht et le prochain responsable du service informatique de Sierre qui pourrait être DPO conseilleraient ainsi les chercheurs
- Un processus de mise en conformité a-t-il débuté ?
  - À ma connaissance non. Si des décisions sont prises par l'institut, il y a un risque de conflit selon les choix des instances dirigeantes → si des recommandations sont faites à l'institut, elles pourraient être contraires à celles de "tout en haut"
  - Donc pas de mesures adoptées avant que les décisions des instances dirigeantes soient prises
- Quelles solutions/mesures concrètes choisies ?
  - Aucune, si ce n'est l'information personnelle
  - Seulement des conseils de bon sens
- Situation actuelle à l'institut, y'a-t-il une distinction avec les projets en Suisse ou en UE ?
  - À ma connaissance, des questions sont posées à l'interne, une prévention est faite, mais pas d'outil et décisions adoptées donc pas de distinction
- Appliquez-vous le principe du "Privacy by design" pour les projets actuels ?
  - Les bonnes pratiques ont été présentées afin de sensibiliser les chercheurs, mais cela reste au stade de conseils
  - Dans la pratique, il faudra vérifier si les chercheurs le font
- Présentation des mock-up réalisés, discussions inputs et outputs, quels besoins et souhaits ?
  - Le type des données devrait pouvoir être mixte
  - Les questions devraient être plus adaptées et moins génériques

ANNEXE 5 Interview IEM

Franceso Cimmino

Phd- Research Assistant Insitut IEM, HES-SO Valais-Wallis

francesco.cimmino@hevs.ch

- Récoltez-vous des données pour vos projets ?

  Oui, pas mal de données sont récoltées.

  Elles peuvent être classées selon 3 typologies : entreprises, résultats d'enquêtes, macro-micro-économiques (brutes).

  Il y a des données personnelles avec les enquêtes, des données sensibles pour les entreprises et également avec les données brutes (santé, préférences de consommation, salaires et classes sociales)

- Quels enjeux pour l'institut IEM ? Quel impact sur les activités ?

  Il devra y avoir une réorganisation, car actuellement il n'y a pas de stratégie commune entre les professeurs.

  Il y a une certitude que les bases de données sont stockées en suisse, mais les droits d'accès sont encore flous (interne, etc.).

  Il n'y a également pas de standards pour les clauses de confidentialité, mais elles sont basées sur les dispositions de l'EPFL généralement.

  La Recherche & Développement devrait être en ordre avec la loi, mais il y a peut-être un vide pour les mandats que nous avons (ils ne sont pas gérés de la même manière avec la HES-SO).

  Les données sont anonymisées seulement quand elles sont publiées, à l'interne elles sont "claires".

- Un processus de mise en conformité a-t-il débuté ?

  Non, il n'y a pas de registre, car pas de vision d'ensemble comme déjà évoqué.

- Présentation et discussion de l'outil

  C'est un bon début. Plus de paramètres pourraient être demandés comme les caractéristiques des données et le nombre de personnes concernées (grandeur du DataSet) ainsi que la source.

  Quelles procédures à mettre en place si le résultat est que le projet n'est pas en règle ? Ne serait-il pas mieux de destiner cet outil directement aux professeurs afin d'éviter une entrevue systématique avec le responsable des données à chaque projet ? (Plus pratique et moins coûteux)

ANNEXE 6 User stories

En tant que…	Je souhaite…	Afin que…
DPO	**Sélectionner un lab**	**Je choisisse celui qui concerne le traitement**
DPO	**Sélectionner un type de données**	**Je choisisse celui qui correspond à mes données**
DPO	**Sélectionner un responsable de traitement, s'il y en a un**	**Je choisisse celui qui concerne le traitement en cours**
DPO	**Avoir une liste de questions selon les textes légaux**	**Je puisse émettre des réflexions sur le traitement de mes données**
DPO	**Avoir la possibilité de répondre aux questions**	**Je sélectionne le choix qui corresponde le mieux au traitement en cours**
DPO	**Visualiser un récapitulatif de mes sélections et choix**	**Je puisse aisément comparer mes résultats avec les sélections et choix que j'ai effectué**
DPO	**Obtenir des résultats selon les 3 périmètres légaux (RGPD, LPD, révision LPD)**	**J'ai la possibilité d'isoler les résultats obtenus selon le(s) périmètre(s) qui me concerne(nt)**
DPO	**Pouvoir recommencer le processus de l'outil à tout moment**	**Je répète le processus pour un autre traitement**

ANNEXE 7 Tâches

Nom	Personne	Date de début	Date de fin	Status	Tags	Heures réalisées
Lectures d'articles	Patrick Clivaz	May 09, 2018	May 31, 2018	Terminée	Etat de l'Art Juridique	22
Rédaction d'une ébauche du cahier des charges	Patrick Clivaz	May 14, 2018	May 17, 2018	Terminée	Cahier des Charges	5
Recherches et analyses outils	Patrick Clivaz	May 21, 2018	May 25, 2018	Terminée	Etat de l'Art Juridique	18
Ajustements du cahier des charges	Patrick Clivaz	May 28, 2018	Jun 07, 2018	Terminée	Cahier des Charges	7
Structure des États de l'Art	Patrick Clivaz	May 28, 2018	Jun 07, 2018	Terminée	Etat de l'Art Juridique,Etat de l'Art Technique	7
Interview T2i	Patrick Clivaz	May 28, 2018	May 28, 2018	Terminée	Etat de l'Art Technique,Etat de l'Art Juridique	2
Rédaction de l'État de l'Art juridique	Patrick Clivaz	May 28, 2018	Jun 18, 2018	Terminée	Etat de l'Art Juridique	40
Rédaction de l'État de l'Art technique	Patrick Clivaz	Jun 11, 2018	Jun 15, 2018	Terminée	Etat de l'Art Technique	15
Rédaction et analyse des choix d'infrastructure et de développemen	Patrick Clivaz	Jun 18, 2018	Jun 22, 2018	Terminée	Analyse et Choix	7
Ajustements des recherches	Patrick Clivaz	Jun 04, 2018	Jun 08, 2018	Terminée	Etat de l'Art Juridique,Etat de l'Art Technique	8
Interview Institut IEG	Patrick Clivaz	Jun 25, 2018	Jun 25, 2018	Terminée	Outil	2
Mock-up et concept de l'outil	Patrick Clivaz	Jun 13, 2018	Jun 14, 2018	Terminée	Outil	9
Structure de la Base de Données	Patrick Clivaz	Jun 12, 2018	Jun 12, 2018	Terminée	Outil	2
Connaissance des technologies	Patrick Clivaz	Jun 11, 2018	Jun 14, 2018	Terminée	Outil,Analyse et Choix	10
Mise en place de la Base de Données	Patrick Clivaz	Jul 03, 2018	Jul 10, 2018	Terminée	Développement,Outil	10
Installation local de l'infrastructure de développement	Patrick Clivaz	Jun 26, 2018	Jun 26, 2018	Terminée	Outil,Développement	4
Création sommaire de la structure du projet	Patrick Clivaz	Jun 28, 2018	Jun 29, 2018	Terminée	Développement,Outil	4
Implémentation graphique	Patrick Clivaz	Jun 26, 2018	Jul 03, 2018	Terminée	Développement,Design,Outil	10
Implémentation technique - Structure MVC	Patrick Clivaz	Jul 02, 2018	Jul 09, 2018	Terminée	Outil,Développement	15
Ajustements techniques	Patrick Clivaz	Jul 12, 2018	Jul 13, 2018	Terminée	Développement,Outil	3
Ajustements visuels	Patrick Clivaz	Jul 17, 2018	Jul 18, 2018	Terminée	Développement,Design,Outil	2
Tests	Patrick Clivaz	Jul 16, 2018	Jul 20, 2018	Terminée	Outil,Développement	4
Finalisation de la rédaction du rapport	Patrick Clivaz	Jul 23, 2018	Jul 27, 2018	Terminée	Rapport	11
Analyse et décisions sur les inputs et outputs de l'outil	Patrick Clivaz,Bruno Montani	Jun 28, 2018	Jul 23, 2018	Terminée	Outil,Etat de l'Art Juridique	30
Rédaction et ajustement du rapport	Patrick Clivaz	May 23, 2018	Jul 23, 2018	Terminée	Rapport	70
Recherches et analyses juridiques	Patrick Clivaz	May 21, 2018	May 25, 2018	Terminée	Etat de l'Art Technique	28
Interview Institut IEM	Patrick Clivaz	Jul 09, 2018	Jul 09, 2018	Terminée	Outil	2
Debriefing juridique et discussion de l'outil	Patrick Clivaz	Jul 11, 2018	Jul 11, 2018	Terminée	Outil,Etat de l'Art Technique	4
Ajustements des inputs/outputs si nécessaire	Patrick Clivaz	Jul 24, 2018	Jul 25, 2018	Terminée	Développement,Outil,Etat de l'Art Juridique	4
Rédaction du guide d'installation locale	Patrick Clivaz	Jul 19, 2018	Jul 20, 2018	Terminée	Rapport	2
						357

ANNEXE 8 Séances

Objectif	Date	Participants	Tags
Première rencontre	Apr 26, 2018 16:30	Patrick Clivaz,Bruno Montani	Introduction
Organisation du Cahier des charges et agenda des séances	May 09, 2018 16:30	Patrick Clivaz,Bruno Montani	Introduction,Cahier des charges
Présentation du Cahier des Charges	May 17, 2018 16:30	Patrick Clivaz,Bruno Montani	Cahier des charges,Product Owner
Ajustement du cahier des charges, structure des États de l'Art	May 25, 2018 14:30	Patrick Clivaz,Bruno Montani	Cahier des charges
Interview T2i	May 28, 2018 17:00	Patrick Clivaz, Adriano Labate	Interview
Définir le périmètre du travail correspondant à la HES-SO	May 30, 2018 14:00	Patrick Clivaz,Bruno Montani	Outil,Cahier des charges
Validation du cahier des charges	Jun 07, 2018 16:30	Patrick Clivaz,Bruno Montani	Outil,Cahier des charges,Product Owner
Présentation du concept de l'outil et de l'organisation du travail	Jun 14, 2018 16:30	Patrick Clivaz,Bruno Montani	Product Owner,Outil
Discussion sur le langage et l'architecture : choix technique	Jun 21, 2018 16:30	Patrick Clivaz,Bruno Montani	Outil
Interview Institut IEG	Jun 25, 2018 10:30	Patrick Clivaz, Alexandre Cotting	Outil,Interview
Discussion sur les inputs et outputs de l'outil et du résultat fourni	Jun 28, 2018 14:30	Patrick Clivaz,Bruno Montani	Outil
Présentation de l'implémentation réalisée et discussion de modification	Jul 04, 2018 15:00	Patrick Clivaz,Bruno Montani	Outil
Interview Institut IEM	Jul 09, 2018 15:00	Patrick Clivaz, Francesco Cimmino	Interview,Outil
Rencontre au sujet du mémoire	Jul 11, 2018 9:00	Patrick Clivaz, Natacha Albrecht	Interview,Outil
Présentation de l'outil réalisé	Jul 12, 2018 14:00	Patrick Clivaz,Bruno Montani	Outil
Validation du travail réalisé	Jul 27, 2018 10:00	Patrick Clivaz,Bruno Montani	Outil
Présentation et discussion de l'outil avec Mme Albrecht	Jul 24, 2018 13:30	Patrick Clivaz,Bruno Montani, Natacha Albrecht	Outil

DÉCLARATION DE L'AUTEUR

Je déclare, par ce document, que j'ai effectué le travail de Bachelor ci-annexé seul, sans autre aide que celles dûment signalées dans les références, et que je n'ai utilisé que les sources expressément mentionnées. Je ne donnerai aucune copie de ce rapport à un tiers sans l'autorisation conjointe du RF et du professeur chargé du suivi du travail de Bachelor, y compris au partenaire de recherche appliquée avec lequel j'ai collaboré, à l'exception des personnes qui m'ont fourni les principales informations nécessaires à la rédaction de ce travail et que je cite ci-après :

- Bruno Montani
- Natacha Albrecht

Chermignon, le 27 juillet 2018

Patrick Clivaz